Draft NISTIR 7711

Security Best Practices for the Electronic Transmission of UOCAVA Election Materials

National Institute of
Standards and Technology
U.S. Department of Commerce

[This page intentionally left blank.]

Draft NISTIR 7711

Security Best Practices for the Electronic Transmission of UOCAVA Election Materials

Andrew Regenscheid
Geoff Beier

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

June 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

[This page intentionally left blank.]

Abstract

This document outlines the basic process for the distribution of election material including registration material and blank ballots to UOCAVA voters. It describes the technologies that can be used to support the electronic dissemination of election material along with security techniques – both technical and procedural – that can protect this transfer. The purpose of the document is to inform Election Officials about the current technologies and techniques that can be used to improve the delivery of election material for UOCAVA voters. This document is part of a series of documents that address the UOCAVA voting. The first NIST publication on UOCAVA voting, entitled NISTIR 7551 A *Threat Analysis on UOCAVA Voting Systems*, was released in December 2008. In addition to NISTIR 7551, NIST has released a draft of NISTIR 7682 *Information Systems Security Best Practices for UOCAVA-Supporting Systems* and will be releasing *Security Considerations for Remote Electronic UOCAVA Voting* and *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting.*

Acknowledgements

The authors of this document, Andrew Regenscheid of NIST and Geoff Beier of CygnaCom, wish to thank the state and local election officials who provided us with UOCAVA election procedures in preparation for this document. In particular, the authors would like to thank the Russell Kasselman, Helen Purcell, Paul Lux, and the Florida Division of Elections staff. Also, the authors wish to thank their colleagues who reviewed earlier drafts of this document, particularly Nelson Hastings, Barbara Guttman, Theresa O'Connell, and Quynh Dang.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: uocava-voting@nist.gov

Table of Contents

1 Introduction

To support State and local election officials in carrying out their responsibilities under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), the Election Assistance Commission (EAC) requested that the National Institute of Standards and Technology (NIST) develop security best practices to assist jurisdictions wishing to use electronic means to send or receive voter registration materials and ballot requests, or to distribute blank ballots to overseas and military voters. Many jurisdictions across the country already use electronic mail for these purposes, and some jurisdictions have begun to use Web sites to distribute or collect this information.

In December 2008, NIST released NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems* [1], which documents the threats to UOCAVA voting systems using electronic technologies for all aspects of the overseas voting process. NISTIR 7551 identifies a number of threats to using electronic technologies to obtain voter registration materials, deliver blank ballots, or return cast ballots, emphasizing the need for implementing strong and comprehensive security controls to mitigate the identified threats. That report concluded that existing widely deployed technology can be used to safely expedite the transmission of voter registration and ballot request materials, as well as blank ballots.

1.1 Purpose and Scope

This document first outlines the basic process for the distribution of election material including registration material and blank ballots to UOCAVA voters. It then describes the technologies that can be used to support the electronic dissemination of election material along with security techniques – both technical and procedural – that can protect this transfer. The purpose of the document is to inform Election Officials about the current technologies and techniques that can be used to improve the delivery of election material for UOCAVA voters.

This document provides security best practices for the delivery and reception of voter registration and ballot request materials, and the distribution of blank ballots to overseas and military voters using electronic mail or Web sites. It does not address casting ballots electronically.

This document is part of a series of documents that address the UOCAVA voting. In addition to NISTIR 7551, NIST has released a draft of NISTIR 7682 *Information Systems Security Best Practices for UOCAVA-Supporting Systems* [2] and will be releasing *Security Considerations for Remote Electronic UOCAVA Voting* and *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting.*

Jurisdictions should consult Draft NISTIR 7682, and other NIST computer security guidelines, for general computer security best practices prior to deploying and using an IT system to support voter registration, ballot request, and blank ballot delivery activities. The security best practices provided in Draft NISTIR 7682 are intended for all IT systems used to support UOCAVA voting, including the activities described in this document. However, this document has a much more narrow focus, looking only at how e-mail and Web sites can be used to support the delivery and reception of voter registration materials, and the electronic distribution of blank ballots. The best practices in this document are intended to extend, not override, the best practices in Draft NISTIR 7682.

Jurisdictions seeking best practices related to election management, including election management for UOCAVA voting, should consult the EAC's *Election Management Best Practices* document [27], as well as their existing best practices for facilitating UOCAVA voting [28].

1.2 Audience

The intended audience for this document is election officials at jurisdictions that are considering the use of electronic mail or Web sites to expedite transmission of voter registration materials and blank ballots. Readers are expected to have a good understanding of any applicable state and local election procedures and regulations that must be followed, but only basic understanding of information technology systems.

These best practices may also be useful to IT support staff charged with deploying, configuring, or maintaining the IT systems used to support the UOCAVA voting related activities described in this document, as well as system developers designing systems for these activities. However, this document identifies many policy issues that must be decided by election officials at each jurisdiction. As this document is primarily intended for election officials, many technical details are left out of this document. The primary resource for technical computer security best practices is Draft NISTIR 7682 [2], along with NIST's existing collection of cyber security standards and guidelines.

1.3 Organization

Section 2 provides an overview of the types of election materials that jurisdictions may wish to send to voters by electronic means, and describes what information is provided in this document to facilitate the secure and reliable transmission of those materials to overseas and military voters. It also provides high-level descriptions of the two Internet-based transmission methods that are considered in this document, electronic mail and Web sites.

Section 4 discusses security best practices for using electronic mail and Web sites to send or receive voter registration and ballot request materials. The section emphasizes the importance of protecting sensitive personally identifiable information that may be recorded or stored by the system, and discusses items that jurisdictions should consider on the issue of voter authentication.

Section 5 covers security best practices for using electronic mail and Web sites to deliver blank ballots to overseas and military voters. The section discusses issues that jurisdictions must consider before deploying electronic ballot delivery systems, including ballot control and tracking, and if voter authentication is required prior to serving ballots. This section considers the use of e-mail to deliver printable ballots, posting blank ballots on Web sites for voters to download, and the use of online ballot markers.

This document provides two appendices with additional information regarding computer security best practices. Appendix A provides a brief overview of general computer security best practices that jurisdictions should follow, mainly from a process perspective. While in many cases election officials will not be the ones implementing the security best practices, particularly technical ones, it is important for officials to understand the roles and responsibilities of election and IT staff for securing the overall UOCAVA voting process. This understanding will help election officials manage the process, and ensure that policy decisions are made and key activities are performed by the proper staff members. Appendix B provides an overview of technical controls for protecting IT systems used to support UOCAVA voting.

2 Overview

2.1 Delivery of Election Materials

Electronic transmission methods can be used to deliver election materials at all stages of the election process. This section outlines different types of election materials that jurisdictions may wish to deliver to their overseas voters using electronic mail or Web sites, and highlights some issues that impact the security controls needed to keep information confidential and unmodified.

2.1.1 Informative Materials

A common way for organizations to use e-mail and Web sites is for the distribution of important announcements. In the case of an election, jurisdictions may make announcements reminding voters of upcoming elections, or asking them to ensure their voter registration information is up to date.

In many cases, the same message will go to all voters. In such cases, the information in the announcement will likely not be sensitive. Disclosure of this information to unintended parties, or even improper modification of these messages, would, in most cases, have a limited impact on the election. As such, this document will not cover best practices for the distribution of these materials. However, ensuring the availability and reliability of these systems is important, and jurisdictions should follow general computer security best practices aimed at protecting their communications infrastructure. NIST IR 7682, *Information System Security Best Practices for UOCAVA Supporting Systems* [2], covers high-level security best practices that would help guard against accidental or malicious threats that would impact system availability.

In some cases, announcements to voters may be personalized, particularly in the case of personalized e-mail messages to registered voters. For instance, an e-mail requesting that overseas voters update their voter registration information may be personalized with each voter's current mailing address. In these instances, jurisdictions should consider that announcement as they would any other voter registration communication (see Section 2.1.2 for further discussion on registration communications). In other cases, jurisdictions should consider the sensitivity of the personalized information on each communication when determining if additional security precautions should be taken.

2.1.2 Registration and Ballot Request

Overseas and military voters must register to vote in their local jurisdictions, as well as provide accurate contact information, such as a postal mailing address. A common method for sending this information is to use the Federal Post Card Application (FPCA) [4], which is a form provided by federal law that permits overseas and military voters to register to vote and request blank ballots. The FPCA is accepted in all states, but some state and local jurisdictions have their own registration materials that are more specialized for their jurisdictions. The FPCA requests several pieces of information from voters that is of sensitive nature. The form requests general information about voters, such as their names, dates of birth, sex, race, and political party preference. It also asks for various forms of contact information, including telephone number, fax number, e-mail address, and postal mailing addresses. The current FPCA also asks for voters' social security numbers[1] and state drivers' license numbers (or other identification numbers), which are among the most sensitive information on the form.

The FPCA is a public form that, when blank, does not contain any personalized information. As such, it requires relatively little protection in transit. However, due to the sensitivity of the information on a completed FPCA, particularly the full or partial social security numbers or identification numbers, completed FPCAs should be protected from unauthorized disclosure or modification when being returned to jurisdictions. Section 3 will identify issues that jurisdictions should consider when evaluating the suitability of e-mail and Web-based return of these materials, and will discuss security controls that jurisdictions can implement to protect this information.

2.1.3 Ballot Delivery

Because Internet transmission does not suffer from the same delays associated with postal mail delivery, e-mail or Web-based delivery of blank ballots can significantly reduce the round-trip transit times. Postal mail delivery to remote locations can take significantly more time than delivery times within the United States. For example, delivery through the military postal system to or from Middle East postal offices takes at least 7-12 days [5].

[1] It should be noted that while the FPCA includes a box for voters' social security numbers, not all states require this information. Some states have customized FPCA forms that black out all but the last four social security numbers, or have instructions for filling out the form which indicate that the full social security number is not required.

Blank ballots typically do not contain any sensitive information that must be protected from disclosure to third parties. However, care should be taken that ballots are reliably delivered to voters without improper modification that could invalidate voters' cast ballots. Section 4 will discuss procedures and technical controls that jurisdictions can use to help ensure safe transmission of ballots.

However, blank ballots may be accompanied by additional personalized information. For instance, some jurisdictions include voter-personalized return identification information that voters are instructed to include with their completed ballots. This information, which may take the form of a bar-code encoding of the voter's name, address and ballot style, can help jurisdictions process returned ballots more efficiently by partially automating some of the data entry steps. A smaller set of jurisdictions send out ballots with tracking information. Section 4.2 discusses issues that jurisdictions should consider when employing these, and other, mechanisms to track and identify ballot materials.

Sections 2.2.1 and 2.2.2 will discuss different methods for electronically transmitting blank ballots, which include e-mailing or posting printable documents, or providing a computerized interface for marking a ballot. It should be noted that electronic ballots, particularly those in the form of printable documents, are very easy to copy and distribute. Jurisdictions that electronically deliver ballots should recognize that they no longer have control over printed ballots. This issue, which relates to ballot accounting, will be discussed further in Section 4.2.2.

2.1.4 Ballot Return

Completed ballots have different security requirements than the types of information described in Section 2.1.3. Completed ballots require protection from unauthorized disclosure and modification, while also preserving ballot secrecy. Due to the nature in which ballots are processed to provide ballot secrecy, it is difficult to detect and recover from problems where information has been modified without the voters' knowledge.

Electronic transmission of registration materials and blank ballots presents fewer security challenges. Blank voter registration forms and ballots are public information, and completed voter registration forms can be protected using techniques common to electronic commerce. The scope of this document is limited to providing best practices for registration materials and blank ballots. However, additional work is being done on electronic transmission of completed ballots. NISTIR 7551 discusses threats associated with electronic transmission of marked ballots, along with some

mitigating security controls [1]. *Security Considerations for Remote Electronic UOCAVA Voting* further discusses threats specific to remote electronic voting over the Internet, and the capabilities and limitations of current technologies for Internet voting [6]. In April 2010, the EAC posted testable requirements for kiosk-based Internet voting systems that are intended to be used in a UOCAVA voting pilot project [3].

2.2 Internet Delivery Options

Information can be quickly and easily transmitted between parties connected to the Internet by e-mail or posting information on Web sites. While both of these transmission methods use the same underlying communications infrastructure, the public Internet, there are important distinctions between the ways these two technologies work, and how they might be used to transmit election materials.

2.2.1 Electronic Mail

2.2.1.1 Overview and Description

E-mail allows an individual to send text and/or files from one computer to another. E-mail is transmitted from the sender's computer to his or her mail server (often operated by his or her Internet Service Provider, or ISP), and routed through a series of intermediate servers and Internet routers before being delivered to the recipient's mail server (often operated by an ISP, workplace or a commercial e-mail service provider such as Gmail or Yahoo).

Figure 1 shows a typical path of an e-mail from an election official's workstation to a voter's personal computer. An e-mail sent from an election official passes through the jurisdiction's e-mail server, which is typically under the control of the local jurisdiction. The e-mail passes over the Internet, typically unencrypted, to a server controlled by the voter's e-mail service provider. In many cases, e-mail must pass through the public Internet once again to reach the voter, as many users have e-mail hosted by someone other than their Internet Service Provider (ISP). This connection may or may not be encrypted, depending on the voter's e-mail provider.

As commonly implemented, email offers little to no confidentiality or integrity protections, and does not guarantee delivery of e-mails to recipients. In many, but not all, cases, senders will receive notification if the e-mail server of the recipient does not accept the message. Some e-mail clients support read-receipts, which are a way to request that the recipient send notification to the sender when an e-mail is read. However, read-receipts are not widely supported, particularly in Web-based e-mail clients,

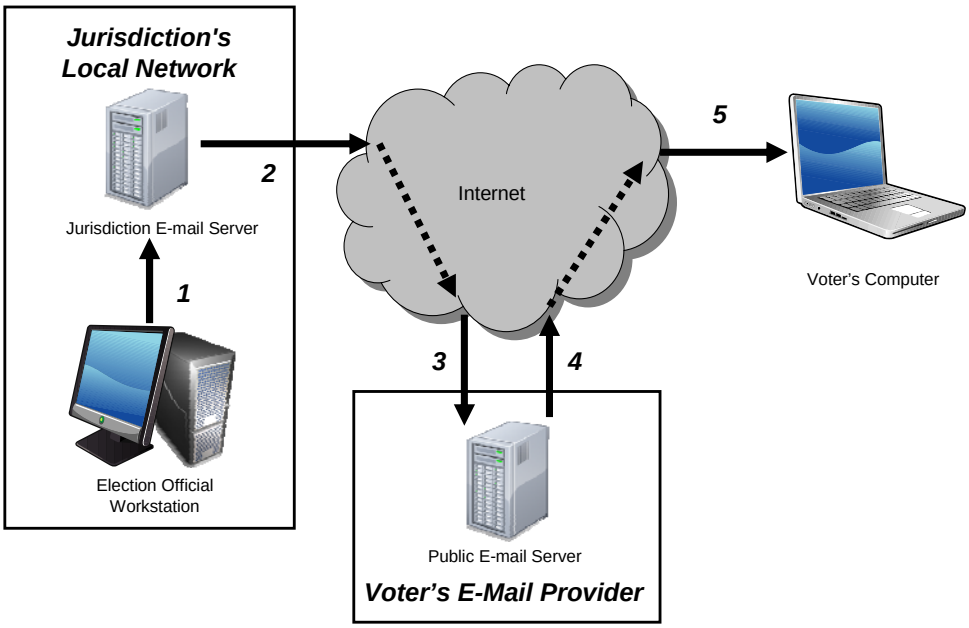

Figure 1: Simplified E-mail Path from Jurisdiction to Voter

and in most cases e-mail recipients must choose to send a receipt back to the sender. Jurisdictions should not rely on read-receipts.

Emails are typically sent unencrypted between the sender and the recipient, and can be read, or even modified, by any legitimate or malicious entity along the email's path, such as both the sender's or recipient's e-mail servers, intermediate email servers or Internet routers, or attackers intercepting traffic. In fact, email servers regularly modify email messages in harmless ways when processing e-mail. Recipients of emails typically cannot confidently verify the originator of an email. In particular, it is very easy for an email sender to forge the "From" field of an email.

Because of the limited security protections offered by email, jurisdictions should not send sensitive information over email, and should discourage voters from sending sensitive information to jurisdictions over email.

- ***Registration and Ballot Request Materials:*** A typical application of email in the UOCAVA voting process is to email attachments (see Section 2.2.1.3) containing blank voter registration forms to voters (e.g., FPCAs), or receive completed forms from voters. However, registration or ballot request information may also be sent directly in an email as text. In both cases, care should be taken that sensitive voter information is not transmitted over email. Section 3.3 describes security best practices for email transmission of voter registration and ballot request materials.

- ***Blank Ballots:*** Email is currently being used by many jurisdictions to send blank ballots to voters. Section 4.3 describes security best practices for email transmission of blank ballots.

2.2.1.2 E-mail Error Messages

Incoming and outgoing mail servers may send error messages to the email sender or originator in the event of some type of error. These take the form of emails from the sender or recipient's email server. Election officials that send emails to voters should be familiar with typical email error messages, but the absence of an error message does not necessarily mean that an email was properly received by the intended recipient.

Emails can fail to be properly delivered to a recipient for a variety of reasons. These include:

- The intended recipient's email address is not recognized (e.g., the intended email account does not exist, the address was mistyped, etc.).
- The outgoing email server is unable to send emails due to a loss of communications of a malfunction.
- The recipient's email server cannot be contacted.
- The intended recipient's email folder is full, and the server will not accept additional emails.
- The outgoing email server, or the recipient's email server, detected a virus
- The email is too large (e.g., due to a large attachment) for either the outgoing email server, or the recipient's email server.

Election officials should read error email messages in their entirety to determine what additional steps to take. For instance, if the outgoing or recipient's email server is down temporarily, the issue may be resolved on its own. However, if the error message indicates that a message was not delivered, the official should attempt to determine why and, if possible, remedy the problem (e.g., use the correct email address). If the problem cannot be remedied, election officials should attempt to contact the voter via some other method.

However, election officials should be aware that some email error messages are sent to the intended recipient, not the sender. For example, if an email is filtered by the recipient's email server due to a detected virus, often that server will only send the error message to the recipient.

2.2.1.3 Attachments

Email messages are often text or HyperText Markup Language (HTML)-based, but can also include one or more files as attachments. While text-

based emails are usually quite small, emails containing attachments can be quite large. Depending on the attachment, an email could grow to be too large for the sender's or recipient's email server. In most cases, emails under 2 megabytes (MB) will be transmitted and accepted by email servers.

Email servers often scan attachments for viruses, and some email servers will reject emails containing attachments of certain file types that often contain viruses. In most cases this should not be an issue for jurisdictions, as typical file types (e.g., .DOC, .PDF, .RTF, .JPG) will be accepted.

2.2.1.4 Email Encryption and Signing

E-mail can be encrypted and digitally signed. The current standards for e-mail encryption and signatures using Public Key Cryptography are the Secure/Multipurpose Internet Mail Extensions (S/MIME) e-mail encryption and signing [7] and OpenPGP [8]. Most major e-mail clients include S/MIME functionality; however use of S/MIME encrypted e-mail is relatively rare. Use of OpenPGP and S/MIME require all users to have a public/private key pair and be part of a Public Key Infrastructure. Furthermore, commonly-used Web-based e-mail providers do not include S/MIME or OpenPGP functionality. Because of the limited deployment and usage of S/MIME and OpenPGP, it is unlikely that these technologies will be practical for securing e-mail communications between election officials and voters. Due to the limited use of S/MIME and OpenPGP, this document will assume that S/MIME and OpenPGP will not be used by jurisdictions or voters. NIST SP 800-45, *Guidelines on Electronic Mail Security*, includes more information about e-mail encryption and signing [9].

2.2.1.5 DomainKeys Identified Mail

The Internet Engineering Task Force recently completed a suite of standards for DomainKeys Identified Mail (DKIM) [10]. DKIM offers a more limited form of email authentication than S/MIME or OpenPGP signatures, but is significantly easier to deploy. The DKIM standards specify a mechanism for email domains (e.g., nist.gov, eac.gov, disa.mil) to sign email and assert responsibility for transmitting the message. When received by a DKIM-aware organization, this information can be used to assign a confidence level to a message through a two-stage process: identity validation; and identity assessment. Identity validation includes verifying the digital signature applied by the originating domain. Once the originating domain has been verified, identity assessment checks if the originating domain is trusted (or checks to what level the originating domain is trusted).

DKIM is generally implemented on incoming and outgoing mail servers, and does not require any special software on e-mail clients. The email servers

sign outgoing messages, verify signatures on incoming messages, and process incoming messages based on the validity of the signature and the level of trust in the originating domain. Because this processing is done on the servers, typically only the email servers need to be part of a Public Key Infrastructure.

DKIM largely verifies the domain of the email, but can provide some assurance of the original sender if one trusts the originating domain to only sign an email after verifying the sender and the email's "From" address. One of the primary applications of DKIM is to help organizations identify, filter, and possibly discard email messages from domains that are not trusted, or known to be untrustworthy (e.g., domains used heavily by spammers or those sending malware or phishing messages).

At this time, DKIM is not yet widely used. However, some email providers have implemented DKIM, including Yahoo, Gmail and FastMail. Jurisdictions should use DKIM to sign outgoing mail and have DKIM-aware servers to process emails to protect themselves from spam and malware, but should not rely on DKIM to verify the original senders of emails.

2.2.2 Web-Sites

2.2.2.1 Overview and Description

Web sites are a popular method for posting information so that anyone with a Web browser can access it. Web sites are collections of pages, graphics, documents, and other digital media that are hosted from a Web server.

All devices connected to the Internet have an assigned Internet Protocol (IP) address (e.g., 172.16.14.128), including Web servers and computers used to access servers. In most cases, users access Web sites using Uniform Resource Locators (URL) containing the organization's domain name, such as http://www.nist.gov. The computers of users accessing a Web page must map these names to the IP address of the server hosting the page by quering the Domain Name System. Figure 2 shows a simplified diagram describing how this works, whereby the user's computer first asks a domain name server for the IP address of the jurisidiction's Web server based on the URL, and then accesses the server.

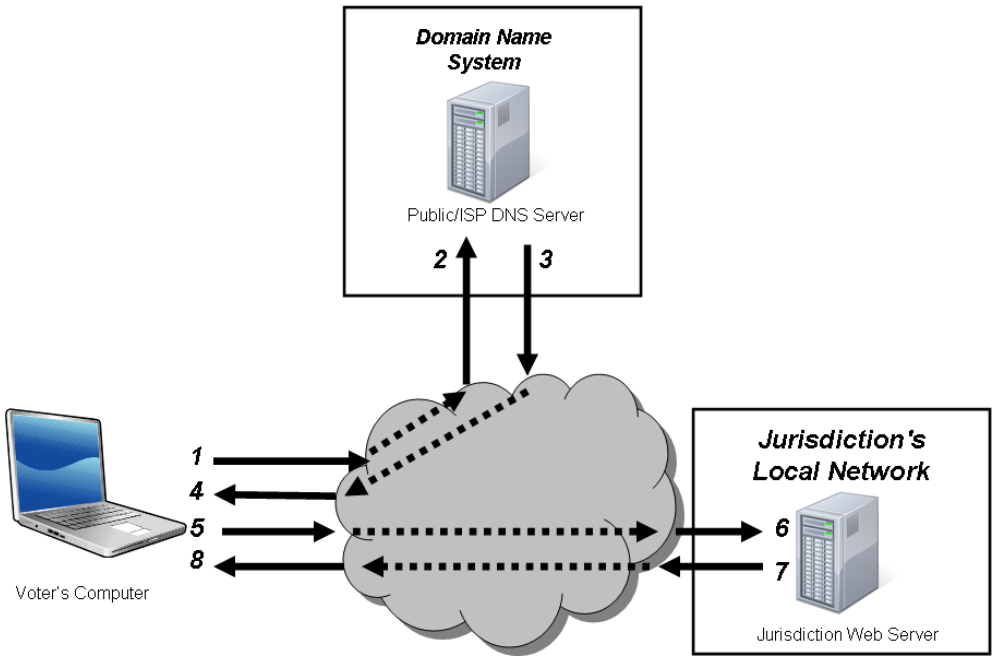

Figure 2: Accessing a Web Page

Attacks on domain name servers, as well as protocols used on the Internet to route messages to the intended destination, can result in messages being intercepted, blocked, or delivered to the wrong party. While efforts are underway to improve the security of these systems and protocols, these attacks highlight the need to use cryptographic protections to ensure users only communicate with the intended parties. There are, however, less sophisticated, but often just as effective, attacks that attempt to trick users into accessing the wrong server. For example, a typical attack on the Internet called Phishing involves tricking a user into clicking on a link to a fraudelent Web site that closely mimicks the legimate site. Such attacks are very difficult to block by technical means.

2.2.2.2 Online File Repositories

Web sites may be used to merely host election-related documents, such as voter registration and ballot request forms (e.g., FPCA) or blank ballots. These sites could be available for all visitors to the site, or access to these forms may be blocked so that only users with a password, or some other authenticator, can access the forms. While Web sites may be more expensive to deploy and use than merely emailing election materials, they do have several advantages. Notably, there are greater security protections possible for delivery of materials over Web sites than over email (see Section 2.2.2.4). Security best practices for posting forms and other

information on Web sites will be discussed in Sections 3.4.1 and 4.4, respectively.

It is also possible for users to upload files to a Web site, as an alternative to email. Again, an advantage to this approach is that Web-based transmission is easier to protect than email transmission. Receiving voter registration or ballot request forms over Web sites will be discussed in Section 3.4.2.

2.2.2.3 Sites with Active Content

Rather than merely posting static Web pages or documents, Web sites often include active content that run as a sort of application in users' browsers. This could take the form of a Web-based form and javascript where a voter enters information, or a Java or Flash-based application that is downloaded by a voter's browser and executed within the browser window.

For example, a Web site supporting voter registration and ballot request could have a Web-based form that allows voters to enter their registration and contact information, and submit it to the election officials. Often Web-based forms will include some logic that helps warn users of mistakes, such as forgetting to include an address or phone number. These sorts of forms are a staple of e-commerce Web sites. Similar forms could be used as a sort of online ballot, allowing voters to make their selections on Web-based form before being presented with a printable marked ballot that could be returned to officials through the mail.

Similar things can be done with Java or Flash-based applications. Rather than being executed by the browser, Java or Flash-based applications are executed by third-party plugins, and displayed within the browser window. Historically, Java and Flash-based applications gave Web developers greater flexibility when programming Web-based applications and interfaces, but advances in browser-based scripting (e.g., Dynamic HTML, Javascript, Ajax) have narrowed that advantage greatly.

Section 3.5 contains security best practices for receiving voter registration or ballot request information using Web sites with active content. Section 4.5 contains security best practices for using these technologies to allow voters to receive and mark a ballot electronically.

2.2.2.4 Transport Layer Security

Transport Layer Security (TLS) [14], and its predecessor, Secure Socket Layer (SSL), are cryptographic protocols that provide confidentiality and integrity protection between a Web server and the client accessing that server. TLS and SSL are widely used on the Internet to provide a safe communications channel for sending sensitive information. For instance,

nearly all e-commerce Web sites use TLS to protect any financial or transaction information sent between the server and user.

TLS is typically used with only server-side authentication, meaning that users connecting to a Web site can verify that they are communicating with the intended entity, but the Web server does not cryptographically verify the users. TLS-enabled Web servers typically have a public key signed by a commonly-trusted certificate authority that allows browsers on users' computers to verify the Web server's identity. However, while TLS is capable of verifying the identity of users (typically called client-side authentication), this requires users to have a public key signed by a trusted certificate authority. This typically is not the case.

TLS is an inexpensive, widely deployed and supported technology, which should be employed by any Web server that sends or receives sensitive information.

2.2.3 Other Delivery Methods

There are a number of other potential mechanisms for sending or receiving election-related materials or information, particularly on mobile devices. For example, Short Message Service (SMS), typically called text messages, are a method for sending short text-based messages to mobile phones. These messages are limited to 160 characters in length, and thus are not likely to be used as a primary communications channel for election materials. However, they may used as a secondary communications channel, e.g., for sending a password or PIN to a user's mobile phone as part of an authentication mechanism.

A fast-growing market on mobile devices is small client-side applications that run on smartphones or other mobile devices. These applications function similarly to applications on a standard personal computer, but many are Internet-connected, and are designed to send information between the mobile device and some Web server operated by the application owner. While browsers on mobile devices are capable of accessing Web sites like any other computer, these small client-side applications are specifically designed to present material in a way that is more appropriate for a small display, as the application can be tailored specifically for the mobile device.

This document will not contain security best practices for these delivery mechanisms, as they are not expected to be used for critical election functions in the near term. However, they are not free of potential security issues. Jurisdictions should carefully consider potential security issues before deploying election-related systems based on these mechanisms.

3 Transmission of Registration/Ballot Request Materials

3.1 Overview

Voter registration and requests for a blank ballot by the UOCAVA voter can be reliably facilitated and expedited by the use of any of the electronic transmission options discussed in this document, including transmission over email and Web sites. However, voter registration and blank ballot material requests can involve transmission of sensitive information, and improper protection in transit, storage and processing can put this information at risk or theft of manipulation, and could impact the ability of voters to successfully cast ballots. This section will cover basic procedural and technical security controls aimed at protecting information related to voter registration and blank ballot materials.

3.2 General Issues

3.2.1 Voter Registration

Jurisdictions must decide how electronically transmitted voter registration information will be used, particularly information electronically returned to state or local election offices. The voter registration process implicitly establishes a trusted relationship that the applicant is an eligible voter in the given jurisdiction. The registration process may involve the transmission or establishment of a trusted authentication token, such as the voter's signature that could be used to authenticate future correspondence from the voter. Depending on a jurisdiction's requirements for voter registration, it may be difficult, or impossible, to send the required information over a desired transmission method (e.g., an original hand-written signature, often called a "wet" signature, over email).

Jurisdictions that are unable to accept electronically transmitted voter registration materials may still be able to accept electronically transmitted materials for updating voter registration information, or requests for blank ballots.

3.2.2 Voter Authentication

Prior to accepting electronically-transmitted election materials from voters, jurisdictions must consider what level and type of authentication they will perform on the materials. This includes the initial voter registration materials, as well as any subsequent correspondence between the jurisdiction and the voter, including updated voter registration information and completed ballots, whether they are sent electronically or physically.

Jurisdictions must decide upon appropriate mechanisms for authenticating voter registration, blank ballot request, and completed ballots. Typically, the initial voter registration application from a voter includes a signature (or a signature is available from other state records, such as DMV records), and future correspondence is authenticated by matching the signature on that correspondence to the signature on file. If a signature is not available, either because a given piece of correspondence may be the first received from a voter, or because previous correspondence did not establish a trusted voter signature, other authentication methods may need to be used, depending on the jurisdiction's desired level of assurance that the material came from the voter in question.

Identification numbers, such as the social security, drivers' license, or passport number, may appear to be convenient mechanisms for voter authentication, particularly as they already appear on the standard Federal Post Card Application (FPCA). However, it should be noted that these are identifiers, not authenticators, and are not designed to be secret. Social security numbers are known by many parties other than the holder, and in some states driver's license numbers are merely an encoding of the holder's name and date of birth. Jurisdictions should carefully consider the use of these identification numbers as authenticators.

E-mail headers and return addresses can not be used for voter authentication purposes. As noted in Section 2.2.1, this information is very easy to forge.

Some jurisdictions require a "wet" signature on file for each voter that can be used to authenticate future correspondence from the voter. That is, an original signature specimen written on a piece of paper, as opposed to a faxed or scanned copy. "Wet" signatures cannot be transmitted electronically, as electronic medium will be digitized copies of a physical specimen. Jurisdictions requiring a wet signature on file may not be able to accept FPCAs or other registration materials electronically when a voter's original signature specimen has not been established, or they may need to update the voter's signature file with some future correspondence sent via postal mail.

3.2.3 Protecting Personal Voter Information

Voter registration and ballot request information will likely contain personally identifiable information. The Government Accountability Office defines personally identifiable information (PII) as "any information about an individual maintained by an agency, including (1) any information that can

be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[23] Election authorities should consult relevant state and local laws to determine if there are governing rules and regulations for PII in their jurisdiction.

Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, or mother's maiden name.
- Personal identification number, such as social security number (SSN), passport number, driver's license number, or financial account number.
- Contact information, such as street address or email address.
- Personal characteristics, including photographic image, handwritten signatures, or biometric data.

Not all PII must be protected equally. Section 3 of NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, identifies six factors that organization should consider when determining the appropriate level of protection. Organizations should consider the following:

- How easily the PII can be tied to specific individuals.
- The number of individuals whose PII is stored in the system.
- The sensitivity of the data.
- The context of how the data will be used, stored, collected, or disclosed.
- Legal obligations to protect the data
- The location of the data, and level of authorized access to the data.

Further guidance on what constitutes PII, factors that influence PII sensitivity, and how PII should be handled from collection to destruction is provided in NIST SP 800-122 [24] or Section 3.3 of Draft NISTIR 7682 [2].

Sensitive forms of PII, such as full or partial social security numbers, should not be sent over the Internet without use of encryption technology. After consulting local, state and federal law, jurisdictions must determine for themselves what constitutes sensitive PII, or whether the factors provided above indicate that a given set of PII may or may not be sent over the Internet without encryption or integrity protections. Jurisdictions should err on the side of caution whenever possible. This may limit the acceptable uses of email transmission of completed voter registration and ballot request materials, as email is typically not sent using encryption. However, it is relatively easy and inexpensive for jurisdictions to encrypt information in-transit submitted from Web sites using TLS.

3.2.4 Preparing Registration/Ballot Request Forms

Voter registration forms that are intended to be emailed or posted on Web sites should be converted directly into a publically-available document format. Suitable public document formats include, but are not limited to, Portable Document Format (PDF) [21] and MS-Word compatible DOC format [22].

Notably, forms should not be merely electronic scans of paper documents. Electronically scanned documents are typically much larger than documents directly saved in an electronic document format, often contain text that is more difficult to read, and are typically not compatible with screen readers.

As noted in Section 3.2.3, forms should not ask for information that is not required or desired by jurisdictions. For example, the standard FPCA asks for a voter's full social security number, but many jurisdictions do not require, or use, this information. Those jurisdictions should remove, or black-out, the box for this information on any forms that they post.

If the publically-available document format supports it, forms should be electronically editable, so that voters may fill in the forms on their computers, even if they intend to print the document prior to return. Many formats have extensions which support scripting languages that can be used to help voters avoid mistakes when filling out forms. For instance, Javascript can be used in the PDF format to warn voters if they miss required questions. In the case of Word-compatible document formats, macros could be used. However, these extensions can cause compatibility problems, and such documents should be tested in popular document viewers. In particular, jurisdictions using these extensions should ensure that the forms work even in document viewing applications that do not support those extensions, or have these features disabled (e.g., Javascript may be disabled in many PDF readers for security reasons).

Some publically-available document formats, including PDF and DOC, support digital signatures. Jurisdictions should consider digitally signing voter registration or ballot request forms prior to emailing or posting them in order to give voters additional assurance that they received the correct, unaltered forms. Additionally, in the case of the DOC format, if macros are used in the document, they can be digitally signed. If the signing certificate is trusted by the system, this increases the likelihood that the macros will be executed in the most common configurations. For these signatures to be effective, jurisdictions must obtain a digital certificate from a widely-trusted certificate authority. The federal "Common Policy" root certificate is now trusted by most current configurations of PDF and DOC processing software. So, if a jurisdiction is affiliated with an organization who has cross-certified

with the federal bridge certification authority, e.g. the State of Illinois PKI, there may be a simple internal channel for obtaining a trusted certificate. Otherwise, jurisdictions will need to purchase a certificate from a commercial authority. This may not be cost-effective, particularly if a jurisdiction does not intend to use the certificate to sign other important electronic documents.

3.3 Electronic Mail

3.3.1 Delivery

Voter registration and ballot request forms should be prepared as described in Section 3.2.4 to ensure the electronic files have the best possible chance of being successfully delivered to voters, and to ensure that they only ask for the information required by the jurisdiction.

Jurisdictions should beware of spam filters which may inadvertently mark their messages as spam and not display it to users. It is difficult to ensure that emails sent by jurisdictions will not be marked as spam. Implementing one of more email authentication technologies, such as DomainKeys Identified Mail [10], Sender Policy Framework [11], and Sender ID [12], may decrease the likelihood of messages being inadvertently marked as spam. Jurisdictions may also consult the Message Anti-Abuse Working Group's *Sender Best Communications Practices* for additional technical measures [13]. One additional measure setup test accounts at popular Web-based e-mail providers and send test message to the accounts to check that they are correctly received.

Outgoing e-mails to voters should be logged, either in the voter registration database, or by some other means. The type of e-mail sent (e.g., voter registration form), the date and time the message was sent, and the official sending the email should be logged.

Automatic Mailings

Jurisdictions may use software to automatically mail voter registration or ballot request forms to registered UOCAVA voters, providing them an opportunity to update their mailing addresses, or renew their requests for absentee ballots.

In this case, the system used to automatically e-mail outgoing forms must be given a list of voters to e-mail voter registration and ballot request material to, and one or more files that will be attached to each outgoing email. Election officials should manually inspect each file prior to loading it on the system to ensure it contains the correct

information. E-mail lists should be deleted from the system as soon as they are no longer needed by the system.

Following transmission of e-mails, the system should provide election officials with a list of any e-mails that could not be delivered, and provide a description of the error encountered when attempting to deliver the message. The system should also indicate whether or not it will attempt to send the message again.

E-mails should be addressed to voters individually, rather than sending a single e-mail to a group of voters. The "Reply-to" and "From" fields of the outgoing e-mail should be set to an e-mail account monitored by election officials.

Manual Mailings

In many cases, voter registration materials will be manually e-mailed to voters from a workstation controlled by an election official. In these cases, the workstation should be configured according to accepted computer security best practices, including using an encrypted connection to the e-mail server for both incoming and outgoing messages. The workstation should be used solely for election purposes.

Generally, e-mails should be addressed to voters individually, rather than to a list of voters. If a single e-mail is addressed to multiple voters, the list of voters' e-mail addresses should be entered in the blind carbon copy (BCC) field, to hide the list of e-mail addresses from the recipients.

Election officials should closely monitor the sending e-mail account for any error messages that indicate a message was not properly received by the voter. Some types of e-mail error messages were described in Section 2.2.1.2. Election officials should read the error message to determine the nature of the problem, and if they need to attempt to communicate with the voter via some other means.

Personalized E-mails

Jurisdictions may wish to send personalized e-mails to voters containing voter-specific information, such as names and current mailing addresses. As e-mail messages are typically not encrypted (unless S/MIME or OpenPGP encryption is used), no sensitive information should be included in the personalized e-mails.

3.3.2 Reception of Forms

Completed voter registration forms collected over e-mail are expected to be received and processed by election officials manually. As with e-mail delivery, workstations used to collect voter registration forms over e-mail should be configured accordingly to accepted computer security best practices, including using an encrypted connection to the e-mail server for both incoming and outgoing messages. The workstation should be used solely for election purposes.

As election officials will be opening emails from voters, and potentially attackers, it is important to properly secure the workstation against possible attacks. While these protections are appropriate for any election workstation, it is critical to ensure that the workstation is running up-to-date antimalware software at all times, and ensure that it is configured to scan incoming e-mail messages. Applications used to open e-mails, or to open email attachments, should also be hardened. In particular,

- Microsoft Office, and other document viewers, should have macros disabled.
- PDF viewers should have any available enhanced security protections enabled, and active content (e.g., javascript) should be disabled.

In case voters choose to send encrypted or signed messages, the e-mail client should be able to process S/MIME signed or encrypted e-mail messages. Most commercially-available e-mail clients include S/MIME functionality by default. This support, combined with successful internal PKI initiatives has led some organizations to enable S/MIME digital signatures by default for email sent from increasing numbers of their systems. Jurisdictions should test their system with signed email, to ensure that the digital signatures do not hamper processing.

Upon receiving a voter registration form the election official should process the form by transferring the required information into the voter registration database and, if required by local procedures, printing a copy of the form. As soon as the voter registration form is processed, the e-mail containing that form should be deleted from both the e-mail client and the e-mail server, as these locations are generally not suitable locations for long-term storage of sensitive personal information. Election officials may wish to save an electronic or physical copy of the received e-mail, including full e-mail headers and attachments, to the voter registration database or other voter management system, to keep as an audit trail.

3.4 Web-Based File Repositories

3.4.1 Delivery

Voter registration and ballot request forms should be prepared as described in Section 3.2.4 to ensure they only ask for the required information from voters. Election officials should manually inspect the contents of the form prior to loading it on the Web server, and all accounts, except for the system administrator, should have read-only access to the form. The server operating system and Web server application should be configured and deployed according to widely accepted computer security best practices.

In most cases, the form should be delivered to voters using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites.

3.4.2 Reception

Jurisdictions may receive completed voter registration forms over Web sites that allow users to upload the completed form to the jurisdiction's Web server. This approach offers greater security than e-mail transmission of voter registration and ballot request forms, notably encryption and integrity protection in-transit using SSL/TLS. However, these protections can be used for Web-based forms, as described in Section 3.5. In most cases, use of online forms will be preferable to uploading completed forms to a Web site, except in cases where a jurisdiction must obtain the voters' signatures.

The Web server's operating system and election application should be configured and deployed according to widely accepted computer security best practices. Files should be uploaded using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites. Uploaded files should not be stored directly on the Web server; rather, they should be received by the Web server, and stored on a system that is not directly accessible from the Internet.

The system should restrict file types users may upload to those commonly used for scanned documents. This includes PDF files, as well as common image formats, such as JPEG, Bitmap, and PNG files. This limits the ability of potential attackers to upload malicious code or other unwanted files, and makes it less likely that voters will upload the wrong file.

The system should set a maximum file size for uploaded files, such as one megabyte. This will limit attackers' ability to enact a denial of service attack by overwhelming the storage capacity of the system.

Uploaded files should not be readable, or executable, by the Web server. This will make it more difficult for malicious individuals to improperly access files uploaded to the server. For instance, without this protection, an attacker may attempt to access voters' voter registration forms. Or, an attacker may attempt to take advantage of the Web server to host illegal material, such as copyrighted material.

Uploaded files should be scanned for malicious code, and the file type verified, prior to making them readable by any other processes or users. File type verification should not merely check the file extension; it should read the contents of the file and verify the file format against the approved list of file formats. This important step attempts to protect workstations accessing these files from attacks involving malicious code.

Election officials should process voter registration and ballot request forms at regular intervals, removing them from the online system as soon as they've been processed.

3.5 Online Forms and Active Content

Jurisdictions may deploy Web sites that allow voters to view or submit voter registration and ballot request materials directly within the Web page. Depending on the functionality of the Web site, the system may or may not require access to current voter registration information, including access to the voter registration database.

3.5.1 Submit Registration or Ballot Request Information

The threat of a data breach exposing personal information is less likely if the Web site only collects voter registration and ballot request information, but does not allow users to view their own information. This is because the read access to this information can be tightly locked down. In this case, the system should not directly connect to the jurisdiction's voter registration database. Instead, election officials should process materials received from voters, and enter the submitted information in those materials into the voter registration database manually, or through a semi-automated process provided by the online system collecting information and the voter registration database.

The Web server's operating system and the election application hosting the vote registration and ballot request form should be configured and deployed according to widely accepted computer security best practices. The Web site should be hosted using the HTTPS protocol using SSL 3.0 or TLS 1.0 or

higher and NIST-approved cipher suites. Information submitted using the form should not be stored directly on the Web server; rather, it should be received by the Web server, and stored on a system that is not directly accessible from the Internet.

As discussed in Section 3.2.2, voters do not necessarily need to be authenticated prior to allowing them to submit voter registration or ballot request information. However, the online form should ask for enough information to allow election officials to have some confidence that a voter is who he or she claims to be. For example, the system could ask the voter to provide some difficult-to-guess information that can be verified against existing voter registration information. In general, the system should perform this verification either in real-time as information is submitted, or before presenting the registration material to the election official. If verification is performed in real-time, the voter should be immediately notified that the verification information was incorrect. If verification is performed at a later time, the system should provide a list of invalid submissions, and allow the official to manually verify submitted information when possible, and follow-up with voters who submitted invalid information.

If verification is not performed in real-time by the system, the Web site should use other mechanisms to attempt to prevent automated attacks whereby an attacker submits a large number of invalid registration changes or ballot requests. An example from e-commerce sites is the use of a CAPTCHA[2] to block automated attacks. CAPTCHAs are little puzzles that users are asked to solve, often involving reading distorted text, to prove that a human is accessing a Web application. CAPTCHAs are often used to try to block attacks where automated computer programs access a Web site and attempt to submit or collect information.

3.5.2 View and Submit Registration Materials

Additional measures to those described in Section 3.5.1 must be taken if Web sites provide UOCAVA voters with the ability to view their current voter registration information. In this case, the Web server requires access to the jurisdiction's voter registration information. However, the system should not have a live connection directly to the jurisdiction's primary voter registration database. Instead, the Web server should connect to a database containing a copy of the jurisdiction's voter registration database that is regularly synchronized with the primary database. Sensitive data fields that will not be used should not be copied into this secondary voter registration

[2] CAPTCHA is a contrived acronym for Completely Automated Public Turing test to tell Computers and Humans Apart.

database. Sensitive data fields that will be used only for authentication purposes should be processed though a NIST-approved cryptographic hash function. This will still allow the application to authenticate the user, but will limit the impact of a data breach should attackers gain access to this database.

Users should be authenticated prior to showing them any voter information. The strength of authentication depends on the sensitivity of the data that will be displayed to voters. In general, highly sensitive data, such as driver license numbers, passport numbers, social security numbers, and other identification numbers, should not be presented to voters. However, the voter's registration status, voting district(s), and, in some cases, current postal or electronic mailing addresses may be displayed. Jurisdictions should use whatever information is available to them, either via voter registration or other state records, to authenticate voters before supplying this information. Multiple consecutive invalid authentication attempts should result in the voter's account being temporarily locked, preventing further access attempts, for a predefined period of time (e.g., 24 hours) or until the case can be reviewed by an election official. The number of allowable invalid authentication attempts should be dependant on the difficulty of guessing the required authentication information. If information is relatively easy to guess, such as the voter's registered zip code or date of birth, is used for authentication purposes, then a lower number of invalid authentication attempts could be used. Information that is more difficult to guess, such as an identification number that was generated randomly by the issuing authority, may allow a higher number of invalid authentication attempts to be used.

Making voter registration materials available online does create privacy concerns. Jurisdictions should carefully consider the advantages and disadvantages of deploying such systems. A report issued by the National Research Council, *Improving State Voter Registration Databases* [26], discusses some of the policy and security issues in Appendix D that should be considered prior to deploying online voter registration systems.

4 Delivery of Blank Ballots

4.1 Overview

As noted in NIST 7551, blank ballot distribution to overseas and military voters can be reliably and securely expedited by using Internet transmission methods, including electronic mail and Web sites [1]. Several states and jurisdictions deliver electronic ballots to overseas and military voters, usually by sending these ballots as e-mail attachments. Security best practices for e-mail transmission of blank ballots are provided in Section 4.3. However, e-mail offers limited confidentiality and integrity protection in-transit, as the required infrastructure to support e-mail encryption and digital signing technologies are not widely deployed or used by the general population. Web-based methods can provide greater confidentially and integrity protections by using SSL or TLS. Web sites could be used to allow voters to download electronic ballots that can be printed and marked by hand, or they provide voters with a Web-based application that can allow voters to make their ballot selections on a computer, and print a marked ballot containing their selections. Best practices for these methods are discussed in Sections 4.4 and 4.5, respectively.

4.2 General Issues

4.2.1 Voter Identification and Authentication

Jurisdictions must determine whether they will require voters to authenticate prior to receiving blank ballots. Voter authentication is not necessary, as cast ballots are authenticated when they are returned, but it is necessary to identify voters in order to provide them with the correct ballot style. It is important to distinguish voter authentication from voter identification. Web-based ballot distribution systems should request sufficient information from a voter to identify the appropriate ballot style. If the information requested is not secret, and is primarily intended to identify the correct ballot style, rather than to restrict access to electronic ballots, it should not be considered an authentication mechanism.

However, for Web-based ballot distribution systems, jurisdictions may still decide to authenticate voters before serving them ballots, particularly when ballots are distributed with information that identifies the voter that will be returned with a completed ballot (see Section 4.2.3 for more information on return identification). Any mechanism used to remotely authenticate voters should serve as a secondary method to authenticate returned ballots, with voter signatures generally providing the primary mechanism to authenticate returned ballots. As such, the strength of the remote authentication method

can be relatively weak as long as jurisdictions are confident in their ability to verify voter signatures.

4.2.2 Ballot Accounting

As part of the ballot accounting process, many jurisdictions keep track of the total number of ballots printed. After an election, jurisdictions can compare the total number of completed and blank ballots with the total number of ballots printed. This is effective for managing ballot stock at polling places, although less so when paper ballots are mailed to voters.

Jurisdictions that electronically transmit ballots generally must accept they no longer have control over who will receive ballots, and how many copies of ballots will be created. Electronic ballots are easy to copy and transmit to third parties.

Jurisdictions that are particularly concerned about unauthorized copying of electronic ballots may put digitally-signed identifiers on each transmitted ballot that would uniquely identify a given ballot. While these ballots could be copied, a third party could not create a new ballot with a different identifier, as the third party could not create a valid digital signature on that identifier. However, placing unique identifiers on ballots introduces potential problems related to ballot secrecy.

A preferable alternative to placing unique identifiers on each ballot is to digitally sign return identification information that must accompany ballots when they are returned, but are separated from the ballots before tallying. This method provides a similar level of protection against unauthorized individuals returning copied electronic ballots.

However, jurisdictions may still find it desirable to place identifiers on ballots in order to track ballots from distribution to tallying. Such identifiers could assist election officials during the ballot reconciliation process. The advantages and disadvantages to using these types of identifiers are discussed in Section 4.2.4, *Ballot Tracking*.

4.2.3 Return Identification

In order to correctly process completed ballots upon return to a voter's local election office, completed ballots are accompanied with return identification information that identifies (e.g., voter name, voter identification number) and authenticates (e.g., voter signature) the voter. The information identifying the voter may be written by the voters themselves, or it can be pre-generated on the materials provided to voters. In the case of postal

mail voting, this information is usually printed on the ballot return envelopes that are delivered to voters with blank ballots. In the case of electronic distribution of ballots this information would likely be printed on sheets of paper that would accompany a completed ballot.

Computer-generated return identification information, whether created by election officials prior to transmission of blank ballots, or by software on voters' machines, can be machine-readable, in the form of barcodes or text printed in a font compatible with optical character recognition. Any machine-readable return identification information should also be available in human-readable form as well, except for information intended to protect the integrity of the machine-readable encoding (e.g., digital signatures, checksums, message authentication codes, or error correcting codes).

As noted in Section 4.2.1, return identification information should never be used as the primary method for voter authentication, but it may be used as a secondary method to complement primary methods, such as verifying voter signatures. In these cases, voters should have to authenticate to a system before receiving the return identification information, such as by authenticating to their private e-mail accounts, or authenticating to the election jurisdiction's online ballot delivery system. Return identification information should be presented in a machine-readable format, and digitally signed using a private key controlled by the election jurisdiction.

4.2.4 Ballot Tracking

Except when required by state law or local election procedures, distributed ballots should not have any identifying information that can be used to link a voter to a particular ballot (e.g., voter name, ballot serial numbers).

However, election laws or procedures may mandate the use of such identifiers. In these cases, systems storing ballot identifiers should protect this information from unauthorized disclosure through cryptographic and other technical means. Ballot identifiers should be automatically generated by the system, and stored in an encrypted format. Depending on legal or procedural requirements, the system should either not provide the capability to link a voter to a ballot, or the system should only supply linkage information after two or more election officials have authenticated to the system.

As an alternative, tracking information can be written on ballot return envelopes or included with return identification information. Tracking information on these items do not pose ballot secrecy concerns, as they are detached from cast ballots before tallying.

In addition, cast ballots may be given tracking information during processing. For example, ballot privacy envelopes could be numbered after separation from the return identification information that identifies the voter. In this instance, care should be taken procedurally and technically so that the numbering of the privacy sleeves cannot be used in combination with other available information to link voters to ballots.

In most cases, jurisdictions receiving paper ballots that were printed by the voter will have to copy the voter's selections on the received ballot on to official ballot stock. In these cases, tracking information should be written to both the original ballot received from the voter, and the transcribed ballot on official ballot stock that links the two ballots. This linkage does not impact ballot secrecy, as the identity of the voter has already been separated from the completed ballot.

4.2.5 Ballot Preparation

Jurisdictions should follow the EAC's existing best practices for ballot preparation, including those describe in the Election Management Guidelines [27] and the Ballot Preparation/Print and Pre-Election testing Quick Start Guide [29].

Blank ballots that are intended to be emailed or posted on Web sites should be converted directly into a publically-available document format. Suitable public document formats include, but are not limited to, Portable Document Format (PDF) [21] and MS-Word compatible DOC format [22]. Notably, due to file size considerations, ballots should not be merely scans of printed paper ballots.

If the publically-available document format supports it, ballots should be electronically editable, so that voters may make their choices on their computers, even though they are expected to print the ballot and sign accompanying forms. As noted in Section 3.2.4, many formats have extensions which support scripting languages that can be used to help voters avoid mistakes when filling out forms. For instance, Javascript can be used in the PDF format to warn voters if they overvote. However, these extensions can cause compatibility problems, and such documents should be tested in popular document viewers. In particular, jurisdictions using these extensions should ensure the forms work even in document viewing applications that do not support those extensions, or have them disabled (e.g., Javascript may be disabled in many PDF readers for security reasons).

Some publically-available document formats, including PDF and DOC, support digital signatures. Jurisdictions should consider digitally signing

voter registration or ballot request forms prior to emailing or posting them in order to give voters additional assurance that they received the correct, unaltered forms. Additionally, in the case of the DOC format, if macros are used in the document, they can be digitally signed. If the signing certificate is trusted by the system, this increases the likelihood that the macros will be executed in the most common configurations. For these signatures to be effective, jurisdictions must obtain a digital certificate from a widely-trusted certificate authority. The federal "Common Policy" root certificate is now trusted by most current configurations of PDF and DOC processing software. So, if a jurisdiction is affiliated with an organization which has cross-certified with the federal bridge certification authority, e.g. the *State of Illinois Digital Signature Project*, there may be a simple internal channel for obtaining a trusted certificate. Otherwise, jurisdictions will need to purchase a certificate from a commercial authority. This may not be cost-effective, particularly if a jurisdiction does not intend to use the certificate to sign other important electronic documents.

If an online ballot marking tool is being provided to voters, constructed ballot definition files should be treated as blank ballots, using technical and procedural controls to ensure the accuracy and integrity of the information on in the files. After loading the ballot definition files in the ballot marking tool system, election officials should test each ballot style within the ballot marking tool, inspecting the candidate and race information.

4.3 Electronic Mail

Blank electronic ballots should be prepared as described in Section 4.2.5 to ensure the files have the best possible chance of being successfully delivered to voters, and contain the accurate candidate and race information.

Jurisdictions should beware of spam filters which may inadvertently mark their messages as spam and not display it to users. It is difficult to ensure that emails sent by jurisidictions will not be marked as spam. Implementing one of more email authentication technologies, such as DomainKeys Identified Mail [10], Sender Policy Framework [11], and Sender ID [12], may decrease the likelihood of messages being inadvertently marked as spam. Jurisdictions may also consult the Message Anti-Abuse Working Group's *Sender Best Communications Practices* for additional technical measures [13]. One additional measure setup test accounts at popular Web-based e-mail providers and send test message to the accounts to check that they are correctly received.

Outgoing e-mails to voters should be logged, either in the voter registration

database, or by some other means. The type of e-mail sent (e.g., blank ballot, replacement ballot), the date and time the message was sent, and the official sending the email should be logged.

Automatic Mailings

Jurisdictions may use software to automatically mail blank ballots to registered UOCAVA voters. In this case, the system used to automatically e-mail ballots must be given a list of voters to receive e-mailed ballots, and one or more files that will be attached to each outgoing email (e.g., ballot, signature card). Election officials should manually inspect each ballot prior to loading it on the system, including checking the candidate and race information, and verifying any digital signature that may be present. E-mail lists should be deleted from the system as soon as they are no longer needed by the system.

The server or workstations sending e-mails should be configured according to accepted computer security best practices, including using an encrypted connection to the e-mail server.

Following transmission of e-mails, the system should provide election officials with a list of any e-mails that could not be delivered, and provide a description of the error encountered when attempting to deliver the message. The system should also indicate whether or not it will attempt to send the message again.

E-mails should be addressed to voters individually, rather than sending a single e-mail to a group of voters. The “Reply-to” and “From” fields of the outgoing e-mail should be set to an e-mail account monitored by election officials.

Manual Mailings

In many cases, blank ballots will be manually e-mailed to voters from a workstation controlled by an election official. In these cases, the workstation should be configured according to accepted computer security best practices, including using an encrypted connection to the e-mail server for both incoming and outgoing messages. The workstation should be used solely for election purposes.

If ballots are manually transmitted to voters by electronic means, such as by e-mailing electronic ballots as attachments or sending e-mails with links to ballots, the sending election worker should verify the correctness of the ballot before transmission.

Election officials should verify blank ballots prior to sending them to voters. If digital signatures are applied to the electronic blank ballots, this should include verification of the digital signature. Election officials should also verify the ballot race and contest information contained on the ballot, and ensure that these match the correct ballot style for the voter.

E-mails should be addressed to voters individually, rather than to a list of voters.

Election officials should closely monitor the sending e-mail account for any error messages that indicate a message was not properly received by the voter. Some types of e-mail error messages were described in Section 2.2.1.2. Election officials should read the error message to determine the nature of the problem, and if they must attempt to communicate with the voter via some other means.

Personalized E-mails

Jurisdictions may wish to send personalized e-mails to voters containing voter-specific information, such as ballot return information or ballot tracking information. This includes information on blank ballots, as well as any accompanying material, such as partially filled in voter signature cards or return envelopes. As e-mail messages are typically not encrypted (unless S/MIME or OpenPGP encryption is used), no sensitive information should be included in the personalized e-mails.

4.4 Web-Based File Repositories

Jurisdictions may post blank ballots on Web sites. This method offers security benefits over electronic mail, as there are widely deployed and used technologies (e.g., TLS) that can be used to protect the confidentiality and integrity of information in-transit.

Blank electronic ballots should be prepared as described in Section 4.2.5 to ensure the files contain the accurate candidate and race information. Election officials should inspect the contents of each ballot prior to loading it on the Web server, including checking the candidate and race information, and verifying digital signatures that may be present. All accounts, except for the system administrator, should have read-only access to the blank ballots. The Web server's operating system and election application should be configured and deployed according to widely accepted computer security best practices.

Voters should identify themselves to the system in order to allow the system to provide the correct ballot to each voter. As discussed in Section 4.2.1, voter authentication is not necessarily required, particularly if voters are not restricted from downloading their ballots multiple times. However, some form of authentication is required in circumstances where voters will receive return identification information that will be used as a secondary voter authentication mechanism when processing return ballots.

Ballots should be delivered to voters using the HTTPS protocol using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites.

4.5 Online Ballot Markers

Section 2.2.2.3 discussed various technologies for implementing Web-based applications for marking a ballot. Options such as Flash and Java require third-party plug-ins that, while widely deployed, are not present or enabled on all personal computers. DHTML, Javascript, and AJAX Web applications are supported in nearly all modern Web browsers, although these technologies are sometimes disabled for security reasons. The Web server's operating system and election application should be configured and deployed according to widely accepted computer security best practices. Voters should interact with Web applications over an HTTPS connection using SSL 3.0 or TLS 1.0 or higher and NIST-approved cipher suites.

The ballot marking tool is a potential source for vulnerabilities in the system. The tool should be developed in accordance with widely accepted best practices for Web application development, being careful to block common Web application vulnerabilities.

The voting system will, in most cases, require access to a voter registration database in order to look up correct ballot styles, denote that voters have received ballots, and, if necessary, support ballot tracking or return identification systems. These lists may be stored on the server, although in many cases the server will query a database server for this information. In either case, jurisdictions should use the criteria provided in Section 3.2.3 to determine appropriate controls to protect personal voter information. When a secondary database is used, it should only contain a copy of the necessary fields from the jurisdiction's primary voter registration database. Sensitive data fields that will be used only for authentication purposes should be processed though a NIST-approved cryptographic hash function, to limit the impact of a data breach should attackers gain access to the database. If the

server hosting the ballot marker application must query a database server, the connection between these components should provide cryptographic confidentiality and integrity protection, such as using SSL/TLS with NIST-approved cipher suites and mutual authentication.

The system will need access to ballot definition files. The ballot definition files should be treated as blank ballots, using technical and procedural controls to ensure the accuracy and integrity of the information in the ballot definition files. After loading the ballot definition files in the ballot marking tool system, election officials should test each ballot style within the ballot marking tool, inspecting the candidate and race information.

As with Web-based file repositories, voters should identify themselves to the system in order to allow the system to provide the correct ballot to each voter. As discussed in Section 4.2.1, voter authentication is not necessarily required, particularly if voters are not restricted from downloading their ballots multiple times. However, authentication is required in circumstances where voters will receive return identification information that will be used as a secondary voter authentication mechanism when processing return ballots.

To protect ballot secrecy, the printable ballot should be constructed using software that runs solely on voters' computers. At no point should the ballot marking application transmit voter selections to the Web-server. However, Web applications may send information about the voter to the Web server, in order to supply proper candidate and race information, and potentially to support return identification and ballot tracking mechanisms.

Printed ballots may contain machine-readable encodings of information on the ballot, such as ballot style, ballot ID, ballot questions and selections. Machine-readable encodings could take the form of barcodes, or text printed in a font compatible with optical character recognition. Machine readable encodings that are not human-readable (e.g., barcodes) should be digitally signed. Any machine-readable ballot information should also be available in human-readable form as well, except for information intended to protect the integrity of the machine-readable encoding (e.g., digital signatures, checksums, message authentication codes, or error correcting codes).

5 Other Resources

EAC Election Management Resources

- Election Assistance Commission. *Election Management Guidelines*. http://www.eac.gov/election_management_resources/election_management_guidelines.aspx
- Election Assistance Commission. *Best Practices for Facilitating Voting by U.S. Citizens Covered by the Uniformed and Overseas Citizens Absentee Voting Act*. September 2004. http://www.eac.gov/research/uocava_studies.aspx
- Election Assistance Commission. *Quick Start Guides*. http://www.eac.gov/election_management_resources/quick_start_guides.aspx

Additional EAC election management resources can be found on the EAC Web site at http://www.eac.gov.

NIST Computer Security Resources

Guidelines

- Draft NIST IR 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010. http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf
- NIST Special Publication 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
- NIST SP 800-60 Rev 1. *Guide for Mapping Types of Information and Information Systems to Security Categories* (2 Volumes). August 2008. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf
- NIST SP 800-53 Rev. 3. *Recommended Security Controls for Federal Information Systems and Organizations*. May 2010. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

- FIPS 199. *Standards for Security Categorization of Federal Information and Information Systems*. February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers, Version 2,* September 2007. http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
- NIST Special Publication 800-123, *Guide to General Server Security*, July 2008. http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
- Draft NIST Special Publication 800-63 Rev. 1, Electronic *Authentication Guideline*, December 2008. http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf
- NIST Special Publication 800-45, *Guidelines on Electronic Mail Security, Version 2, February 2007*. http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf
- NIST Special Publication 800-122*, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010. http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf

Other NIST Resources

- National Checklist Program (NCP). http://checklists.nist.gov/
- National Vulnerability Database (NVD). http://nvd.nist.gov/
- Security Content Automation Protocol (SCAP) Specifications. http://scap.nist.gov/

A wide range of additional computer security resources are available on the NIST Computer Security Resource Center Webpage at http://csrc.nist.gov/.

Federal Voting Assistance Program (FVAP) Resources

- FVAP. *United States Postal Service Mail Guidelines*. http://fvap.gov/leo/usps-mail-guidelines.html
- FVAP. *Fax & E-mail Guidelines.* http://fvap.gov/leo/fax-email-guidelines.html
- FVAP. *Guidelines for the Help America Vote Act.* http://fvap.gov/leo/hava-guidelines.html

The Federal Voting Assistance Program has set up a portal for election officials to obtain UOCAVA voting-related information and resources at http://fvap.gov/leo/index.html.

Other

- Overseas Vote Foundation**.** https://www.overseasvotefoundation.org/
- Washington Secretary of State. *Ballot Tracking Systems Report to the Legislature*. January 2007. http://www.sos.wa.gov/documentvault/BallotTrackingSystemsReportJanuary2007-1852.pdf
- Oregon Secretary of State. *Vote by Mail Procedural Manual*. May 2010. http://www.sos.state.or.us/elections/vbm/vbm_manual.pdf
- State of Indiana. *Military and Overseas Voter Guide*. 2004. http://www.eac.gov/election/practices/uaoc

6 References

[1] National Institute of Standards and Technology Interagency Report 7551, *A Threat Analysis on UOCAVA Voting Systems*, December 2008.

[2] Draft National Institute of Standards and Technology Interagency Report 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010.

[3] EAC. (2010). UOCAVA Pilot Program Testing Requirements, March 24, 2010. Accessed May 10, 2010 at http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program

[4] FVAP. (2010). Federal Post Card Application. Accessed May 10, 2010 at http://www.fvap.gov/resources/media/fpca.pdf

[5] Testimony of Bob Carey, Director of FVAP. (2010) EAC Public Meeting, Dec. 3 2009. Accessed April 5, 2010 at http://www.eac.gov/public_meeting_12032010/

[6] Hastings, Nelson, Rene Peralta, Stefan Popvenuic, and Andrew Regenscheid. *Security Considerations for Remote Electronic UOCAVA Voting*. Draft Whitepaper for the Technical Guidelines Development Committee. June 2010.

[7] Internet Engineering Task Force. (2010). S/MIME Mail Security. Accessed April 5,2010 at http://www.imc.org/ietf-smime/

[8] Callas, J., Donnerhacke, L., Finney, H. and R. Thayer, "OpenPGP Message Format", RFC 2240, November 1998.

[9] NIST SP 800-45 Version 2. Guidelines on Electronic Mail Security, February 2007

[10] Hansen, T., et. al., "DomainKeys Identified Mail (DKIM) Development, Deployment, and Operations", RFC 5863, May 2010.

[11] Sender Policy Framework (2010). Project Overview. Accessed June 18, 2010 at http://www.openspf.org/

[12] Lyon, J., and M. Wong, “Sender ID: Authenticating E-mail”, RFC 4406, April 2006.

[13] Messaging Anti-Abuse Working Group. (2010). MAAWG Sender Best Commmunications Practices Version 2.0. Accessed June 18, 2010 at http://www.maawg.org/sites/maawg/files/news/MAAWG_Senders_BCP_Ver2.pdf

[14] Dierks, T., and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.1”, RFC 4346, April 2006.

[15] NIST SP 800-60 Rev 1. Guide for Mapping Types of Information and Information Systems to Security Categories (2 Volume). August 2008.

[16] NIST SP 800-53 Rev. 3. Recommended Security Controls for Federal Information Systems and Organizations. May 2010.

[17] Draft NIST SP 800-128. Guide for Security Management of Information Systems. March 2010.

[18] Draft NIST SP 800-34 Rev. 1. Contingency Planning Guide for Federal Information Systems. October 2009.

[19] FIPS 199. Standards for Security Categorization of Federal Information and Information Systems. February 2004.

[20] "Uniformed and Overseas Citizens Absentee Voting Act", P.L. 99-410

[21] ISO 32000-1:2008, Portable Document Format—Part 1: PDF 1.7.

[22] Microsoft. (2010). Microsoft Office File Format Documents. Accessed May 10, 2010 at http://msdn.microsoft.com/en-us/library/cc313105.aspx

[23] GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008.

[24] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.

[25] Federal Trade Commission. (2008). FTC Consumer Alert: FTC Cautions Consumers About Voter Registration Scams. Accessed May 10, 2010 at http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt076.pdf

[26] Committee on State Voter Registration Databases; National Research Council. (2010). Improving State Voter Registration Databases. Accessed June 3, 2010 at http://www.nap.edu/catalog.php?record_id=12788

[27] Election Assistance Commission. (2010). Election Management Best Practices. Accessed June 18, 2010 at http://www.eac.gov/election_management_resources/election_management_guidelines.aspx

[28] Election Assistance Commission. (2004). Best Practices for Facilitating Voting by U.S. Citizens Covered by the Uniformed and Overseas Citizens Absentee Voting Act. Accessed June 18, 2010 at http://www.eac.gov/research/uocava_studies.aspx

[29] Election Assistance Commission. (2006). Quick Start Guide: Ballot Preparation/Printing and Pre-Election Testing. Accessed Jun 18, 2010 at http://www.eac.gov/resource_library/default.aspx?DocumentId=131

Appendix A: General Computer Security Best Practices

A variety of system components will play a role in transmitting election materials electronically. Some of these components will likely serve multiple functions within a jurisdiction, and most are likely to be managed by technical personnel who also maintain IT systems which are unrelated to the transmission of election materials. Close coordination will be required between election officials and technical personnel to ensure that sufficient process and technical controls are in place for the secure deployment of such a system.

Security requirements for systems that contain election materials will differ according to local regulations and practices as well as according to the nature of the materials contained on the system. Even so, certain basic practices need to be followed to secure any important IT system.

This section outlines those general best practices and will help election officials understand the points of coordination required for a secure, functional system. Once the security objectives are identified as part of the system characterization process, a set of security controls will be established to meet these objectives. Some of the controls will be common to many or all systems within the organization, and some may be specifically deployed in support of the election system.

A.1 System Characterization

The first step in securing any system is the establishment of security objectives. In order to select appropriate security measures, election and IT personnel need to have a common understanding of the confidentiality, integrity and availability requirements for the system's data and functions. This requires a thorough description of the system's purpose, data, components and boundaries.

Election officials should work with technical staff to identify or create documentation of the purpose and scope of every system. The resulting characterization will drive planning for fulfilling the system's security objectives. For example, a system whose purpose is delivering information on application deadlines may contain only public domain information that is readily available through other channels, and therefore would not have any confidentiality requirements, might have moderate integrity requirements, and low availability requirements. A system that allows voters to view and modify their registration information might introduce moderate or high confidentiality requirements, depending on the sensitivity of the information displayed.

A.1.1 Functional Description

As a first step to characterizing the system, each function provided by the system must be defined along with who will access that function. In most cases, any technical details expressed in the functional description should be very high-level. For example, election officials may be able to load ballot configuration files on a system, or voters may be able to update their voter registration information on the system. For each function provided by the system, assess the risk posed by failure to provide it. In assessing this risk, it is important to consider legal and procedural requirements unique to the jurisdiction, as these will influence and may even explicitly define the impact of unavailability for some election-related functions.

A.1.2 Data Categorization

In order to provide the functions documented in the functional description, the system will require access to various types of data. Determine what data must be stored on or processed by the system in order to provide each function. Here also, any technical details expressed in the data characterization will be very high-level. Each type of data should be described according to confidentiality, integrity, and availability requirements. For each, establish the impact of improper disclosure, modification or destruction of that data. As with availability of system functions, each jurisdiction may have specific circumstances or legal requirements that help determine this impact. NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* [15] details preliminary characterizations for certain types of data, which may provide a useful starting point. For all other data, this document provides readers with a list of common considerations to use when determining impact levels.

As a general best practice, systems should not store or access any data beyond that which is required to provide an election function identified in the functional description if that data has any confidentiality or integrity requirements.

A.1.3 System Architecture

The description of the system architecture will contain more granular technical details than either the functional description or the data categorization. Election officials should work with IT personnel to describe the components (e.g. servers, routers, workstations) that will be used to deliver the system functions previously enumerated. It is important to understand the role of each component in delivering the system's functions along with what data will be stored in or processed by each. The system

architecture description should account for how component failures could compromise availability, confidentiality or integrity.

All physical and logical boundaries should be established in the system architecture. These should include both technical and organizational considerations. So, for example, any common resources shared across boundaries (e.g. network storage used for both election and other county data) should be identified so that sufficient technical and procedural controls can later be defined.

A.2 Identification of Common Controls

The IT system deployed to support the transmission of election materials will most likely be one of many systems managed by the jurisdiction. In this case, the organization responsible for the operation of the IT systems will have established certain common security controls that apply to all systems and hosting facilities controlled by that organization. These controls should be analyzed in conjunction with the security requirements established during the system characterization for the election system. Election officials should work with the IT management organization to understand which common security controls exist. Together, they should identify both how these common controls can be used to support the voting system security requirements and where new controls need to be deployed along with the new system.

Because system management services will most likely be shared with non-election systems, certain management policies will most likely be common across the organization. Several of these are relevant to system security and merit specific consideration in the context of a system used to process election data:

- Personnel screening is the process by which the organization determines that individuals are suitable for performing specific duties. Election officials should ensure that this process complies with any relevant regulatory requirements governing personnel with access to the types of data identified in the data characterization.
- Configuration Management is the set of policies and processes for controlling system and documentation modifications. Related controls are discussed in detail appendix A.4.
- Contingency Planning is the set of policies and processes intended to maintain and restore election operations in the event of emergencies, failures or disasters. Related controls are discussed in further detail in appendix A.5.

- Physical Access Controls are policies and procedures that govern how personnel gain physical access to systems and facilities. For some components of the system, physical access may imply access to election data which should be identified in the system architecture. Election officials should confirm that the organization's physical access controls on such components are sufficient to meet local requirements.
- User Identification and Authentication controls govern how the system determines a user's identity. The technical details of using these controls to verify identity claims are discussed in NISTIR 7682 [2] and are outside the scope of this document. Election officials should examine the process the organization uses to issue the credentials used for user identification for those users who might have access to sensitive system data and confirm that this process meets applicable regulatory requirements.
- Hardware and Software Acquisition channels are likely to be shared across the organization. Election officials should confirm that this process meets any election-specific requirements.
- Incident Response Procedures are intended to detect, respond to, and limit consequences of IT security compromises. These are discussed in greater detail in appendix A.6.

Certain technical controls are also frequently applicable on a facility-wide basis and therefore tend to be shared by many unrelated systems. These include:

- Physical/environmental aspects of the facility such as availability monitoring, backup power supplies, fire suppression, and media storage.
- Local and remote network access for jurisdiction personnel.
- Network Infrastructure Protections, such as those described in the Appendix.

In addition to common security controls, many jurisdictions will use existing network infrastructure to service some of the functional requirements for the election system. For example, some systems existing as DNS servers, email servers or Web servers will likely be used. Just as with components specific to the election system, the architecture description developed during the system characterization should identify functions provided by and data processed by or stored on the shared components. For this shared infrastructure, election officials should coordinate with those systems' managers to ensure that the system-specific controls are sufficient to meet the security objectives defined for those functions and data.

A.3 Network and Communications Protections

Even with effective security controls configured for those hosts which provide election-related functionality, certain network and communications infrastructure protections need to be in place to support the secure operation of the overall system. In many cases, the network infrastructure owned by a jurisdiction may be used to support both election and non-election functions. The system architecture description developed during the system characterization should identify security objectives for the shared components. Election officials should work with IT management to examine the protections in place on these shared components and ensure that they are adequate to provide the required availability, confidentiality and integrity guarantees for the election system.

Appendix B provides a more detailed discussion of proper network and communication protections that are appropriate for use with a voter registration, ballot request, or blank ballot delivery system.

A.4 Configuration Management

Any IT system that provides a mission-critical function for an organization should have a formal, documented set of policies and procedures for security configuration management. In many cases, the policies will not be system-specific, but will be organization-wide. Existing policies and procedures should be examined and assessed to determine whether they are adequate for meeting the security objectives of the election system or whether system-specific augmentations are required. Whether or not the policies and procedures need to be changed, election officials need to be identified as stakeholders in the configuration management process and play an active role in planning and validating configuration changes.

NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations* [16], details Configuration Management controls that may be appropriate to differing levels of security objectives, and NIST SP 800-128, *Guide for Security Configuration Management of Information Systems* [17], describes how specific parts of the configuration management process support these controls.

A.4.1 Configuration Management Planning

Election officials should review the plan for managing the security configurations of systems that will be used to support the transmission of election materials. Although the IT management organization will generally own the plan, as stakeholders, election officials should review the plan at a high level to ensure that it includes:

- Well-defined roles and responsibilities for personnel involved in proposing, testing, approving and implementing configuration changes
- A description of how configuration items are selected for management control
- A process for establishing a secure baseline configuration
- A process for managing updates to the baseline configuration

In many cases, if an organization has a mature, formal configuration management plan in place, the only augmentation required will be the addition of election officials to key planning, approval and testing roles.

A.4.2 Secure Baseline Configurations

A secure baseline configuration is a documented set of specifications for a system or component that has been reviewed and agreed upon by the stakeholders of a system. The secure baseline configuration can only be updated by following the process outlined in the secure configuration management plan, and should always reflect the state of the current system.

IT organizations are likely to have secure baselines that apply to many components of a particular type (e.g. fileservers). These configurations may then need to be supplemented to meet the security requirements established during the system characterization. The system architecture description should identify each component of the system along with the functions it provides and data it stores or processes. Election officials should work with technical personnel to review each component against the standard secure baseline configuration and determine whether the security objectives are met by the baseline, or to develop a new baseline specific for the election system.

All configurable components which play a role in maintaining the security or availability of the system should have secure baseline configurations.

A.4.3 Change Control

Change control is the documented process by which configuration changes are proposed, justified, implemented, tested and reviewed. Every organization needs to have a change control process which applies to all components involved in the transmission of election materials. This should include changes made to hardware, software, operating systems and applications. Election officials need to ensure that they are involved in the testing and approval of changes that could impact the security or availability of these systems.

Jurisdiction-specific regulatory and procedural requirements may influence the level of scrutiny and approval required for system changes. Election

officials should verify that the change control process meets their jurisdiction requirements.

A.5 Contingency Planning

Contingency planning refers to the collection of plans, procedures and technical measures which will be used to ensure continued availability of system functions in the event of potentially disruptive events. This covers a broad scope of planning activities aimed at ensuring resiliency of system functionality. Election officials should work with technical staff to ensure a solid mutual understanding of system availability requirements and gain assurance that adequate contingency plans are in place.

In most cases, contingency planning activities will cover all critical systems managed by an IT organization and hosted in a particular facility. Election officials should consult with technical staff to ensure that the plans in place are commensurate with the availability requirements described in the system characterization documentation, and that these plans do not compromise the confidentiality or integrity requirements established for the data. So, for example, if local requirements state that access to voter records must be logged, officials should ensure that access to off-site backups containing voter records is similarly logged. NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems* [18], gives examples of contingency planning strategies that map to the impact levels described in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* [19].

A.5.1 Preventative Controls

Preventative controls are established in advance of an event and are aimed at preventing that event from causing a disruption to system functionality. Examples of these controls include short-term, and possibly long-term, backup power supplies, duplicate or backup communication lines, fire suppression systems and regular preventive maintenance. These preventive controls should be commensurate with system availability requirements. In most cases, the fact that a system transmits election data will not impart special requirements for preventive controls in a facility that houses other mission-critical systems.

A.5.2 Backup and Recovery Strategies

Backup and recovery strategies cover those plans and procedures used to restore system operations following a service disruption. Election officials need to understand the allowable downtime for their application and work with technical staff to develop a backup and recovery plan which can restore service without exceeding that threshold. One practice common to all backup

approaches is storage of backup data at a location distinct from the live system.

Backup and recovery strategies need to address outages caused by events from a variety of failures, from simple equipment failure to major natural disasters. Recovery strategies from major long-term failures will rarely be system-specific. For more localized disruptions, there is a substantial advantage to using standard hardware across the IT organization where possible and ensuring that enough spare equipment is available to quickly replace the system and restore the software and data on the system using the backup media. In addition to standardizing equipment and verifying the availability of spares, election officials should ensure that backup hardware is acquired for any election system-specific equipment that could cause an outage to exceed the availability requirements in the event of a failure.

A.5.3 Plan Testing

Contingency plans need to be tested according to availability requirements established when characterizing the system. The goal of testing is to ensure the availability targets are maintained. Election staff should work with IT staff to participate in the tests. This provides the opportunity to confirm that all roles and responsibilities are identified and well understood, prior to an actual disaster. The organization's contingency plan should provide for regularly scheduled testing and should define events that trigger a new test exercise (e.g. turnover of key personnel, facility change, etc.).

A.6 Incident Response

Jurisdictions should ensure that a computer security incident response plan is in place prior to system deployment. Both election officials and IT personnel will have key roles in the incident process.

The incident response plan should clearly define which systems are covered and what constitutes a security incident for each one. Any system involved in the transmission of election data should be covered by an incident response plan. There should be a process for defining an incident's severity and establishing the priority for responding to that incident. Jurisdiction officials should have input into the criteria for severity and priority.

Roles, responsibilities and authority should be clearly documented for various classes of security incidents. Individuals should be identified, and the plan should include details of on- and off-hours communications channels to be used according to incident severity and priority. The plan should also establish a process for approving discontinuation of service in the event of an ongoing incident. Both IT and election representatives will need to be

involved in this process. In most incident response plans, because the initial response will focus on halting an active incident and preserving evidence for later analysis, the initial response will primarily be handled by the technical staff charged with operating and monitoring systems. After the incident, election representatives are likely to have a more central role, as decisions will need to be made on technical or procedural changes to the system as service is restored. Election officials will need to be familiar with any local, state or federal requirements governing notification of affected individuals in the event of a data breach.

Election officials should ensure that the incident response plan addresses any specific legal issues that arise from the nature of the system. For example, some states have specific disclosure procedures that need to be followed in the event of compromise of Personally Identifiable Information.

As with contingency plans, incident response plans should be tested prior to system deployment and periodically thereafter.

A.7 Continuous Monitoring

All security controls should be assessed prior to system deployment. For critical systems, a subset of management, operational and technical security controls should be continuously monitored in several ways, all with the goal of ensuring that system security and availability objectives are met on an ongoing basis as operations continue. Many IT organizations may include continuous monitoring provisions in various plans and policies rather than consolidating these activities under one plan.

Automated network and system monitoring tools should be used and monitored to detect integrity or confidentiality breaches. These tools may monitor log files, network traffic, file changes, etc. IT organizations should have a documented process for responding to output from these tools.

Network and host configurations should be periodically inspected and assessed to ensure they are compliant with current secure baseline configurations. This should involve both automated testing using some combination Security Content Automation Protocol (SCAP)-based tools and the automated system monitoring tools for other purposes and periodic audits. In particular, election officials should ensure an individual is identified and tasked with reconciling log entries which identify security-relevant system configuration changes with configuration management records. This is intended to ensure no change is made to the system without following the required testing and approval process established in the configuration management plans. IT staff should identify which configuration settings can

be automatically monitored and which require manual action by the auditor to inspect the settings and confirm that they match the most recent configuration management records for the deployed system.

Election officials should verify that the IT department identifies an individual or a team tasked with monitoring for public reports of vulnerabilities in the components that comprise the system, as well as common components that serve to support the system. This enables the organization to respond to potential vulnerabilities even in the interval between public disclosure and vendor response.

The continuous monitoring plan should provide for periodic security testing. Some tests can be conducted using only automated tools, which is both inexpensive and beneficial to all the systems managed by the jurisdiction, not solely those used to support elections. Other security tests require specialist expertise which is both quite costly and frequently system-specific. Election officials should work with the IT organization to prioritize and schedule tests according to the impact of a potential security breach on the system.

If any of these mechanisms detects an exception, the monitoring plan should include a process for assessing whether or not the exception is also a security incident. If it meets that definition, the incident response plan should be invoked. Otherwise, there should be a flaw remediation plan in place for reporting and addressing the issue, and updating the secure baseline configuration if necessary.

The continuous monitoring process should be periodically tested, to ensure that exceptions are properly flagged and remedied by the organization.

Appendix B: Component Security Considerations

This appendix offers security considerations for specific components likely to be used in the delivery of election materials to voters, such as network infrastructure, Web servers, email servers and email clients. This is not intended to be a comprehensive guide to all security considerations inherent in configuring such components. Rather, it seeks to reference other materials and identify considerations that are likely to pertain to these system components when they're used to transmit election materials and to guide election officials in collaborating with technical staff to ensure that components are configured and operated in a manner consistent with the security objectives of the system.

This appendix is directed toward readers with a high-level technical understanding of the components used to deliver the business functions of the system. It should assist such a reader in interacting with the technical personnel charged with implementing and managing the system. Prior to considering the guidance in this appendix, the reader should understand the System Characterization and the resulting security objectives.

The information in this appendix is intended to supplement, not replace the best practices in NISTIR 7682. The security practices discussed in that document are critical for all of the systems discussed here. This information is intended only to help the reader better understand the application of those practices for this purpose.

Decisions about which technical controls and protections apply to various system components are driven by the system characterization. Some of these protections will be common, applied to every system the IT organization operates. Others may be specific to components of systems used to deliver election materials. Election officials and technical staff will need to identify areas where existing controls may need to be augmented in order to comply with relevant federal, state and local regulations for protection of the information stored on or accessible via these systems.

The system characterization will have defined the components necessary to fulfill its intended functions. In general, secure deployment of these systems implies that they do exactly what's specified in the characterization and no more. This means that the systems should only store the minimum amount of data necessary to perform their function, only be connected to those other systems required by the characterization, and only be accessible by those individuals who are authorized to have access.

B.1 Network Infrastructure Protections

B.1.1 Establishing Security Boundaries

The system architecture and security objectives produced during the system characterization can then be used to identify specific network infrastructure components and their roles in protecting the system. These components (routers, switches, hubs, firewalls, etc.) can then be classified. Election officials should work with technical staff to identify the security controls which are active for these components, and confirm that these are sufficient to maintain the system's overall security objectives. This enables the establishment of boundaries to control the flow of sensitive information.

The system architecture should be analyzed with an eye toward information flow. Each information object that traverses a piece of network infrastructure should be identified along with the security requirements for that information and the security controls in place for that infrastructure. Information should only traverse network infrastructure with controls sufficient to protect it. If information needs to be sent through infrastructure without sufficient controls to protect it (for example, PII needs to be sent across an organization's general business network) additional measures, such as encryption should be identified and put into place. Threats to information and measures which address those threats are identified in detail in section 3 of NISTIR 7682. Technical protections for network infrastructure are addressed in section 4 of NISTIR 7682.

Components with differing security requirements should be connected to physically distinct networks when feasible. For example, a jurisdiction's Web server and voter registration database will generally have incompatible confidentiality requirements. Ideally, these should not be connected to the same network infrastructure. In many cases such an "air gap" will be impractical or even impossible, due to business considerations. In such cases, additional network protections such as firewalls and application proxies should be used to enforce logical separation at these boundaries.

The business and technical teams need to collaborate to devise rules for exactly what information should be allowed across these boundaries and configure the network protections accordingly. So, for example, two unrelated systems that need to be collocated for budgetary reasons but have no need to share data with each other might be placed onto separate Virtual LANs (VLANs) using a managed network switch. A public server that needs access to portions of a protected database of record might be granted limited access to that database using firewall rules and a back-end application server.

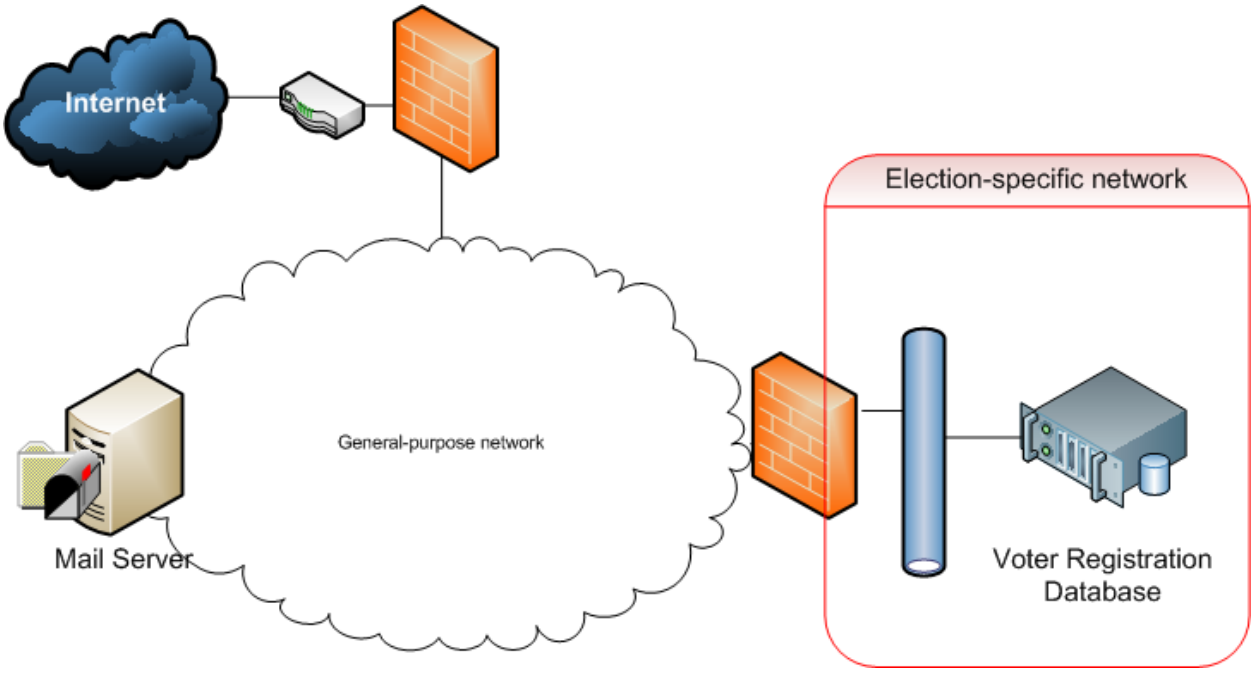

Figure 3. Segmenting election-specific infrastructure from the general-purpose network

B.1.2 Considerations for Shared Infrastructure

In most cases, some components of the system for transmitting election information will support multiple systems. The security-relevant functionality of these shared infrastructure components should be identified. The jurisdiction and the IT organization should work together to understand the security controls that are in place for the existing infrastructure, and evaluate whether these match the security requirements for the election system. For example, on most systems, a compromised or incorrectly configured DNS server, switch or router could cause emailed ballots to be improperly delivered, or grant an attacker the ability to alter them in transit. In such a case, security controls on these shared components should be analyzed against the security objectives of ballot delivery. Election officials should verify that the controls on security-critical shared components meet the security objectives identified for all election-specific functionality that depends on these components. So, in the example above, configuration controls need to meet the security objectives identified for email availability and integrity.

Components that are likely to be shared include Web servers, email servers, DNS servers, workstations, switches, firewalls and routers. Web servers and email servers are discussed in more detail in later sections of this appendix as well as in NISTIR 7682 and in Special Publications 800-44 and 800-45,

respectively. Workstations are discussed in the context of email clients later in this appendix and more generally in NISTIR 7682. For detailed guidance on DNS security, see SP 800-81. Best practices for securing all of these infrastructure components are covered in NISTIR 7682.

Both election and IT stakeholders should ensure that common controls discussed in section 3.2 are considered for all shared infrastructure.

In cases where it is impractical to apply protections required by the sensitivity of the election system to the general-purpose infrastructure, jurisdictions should consider deploying dedicated infrastructure components in support of the election application.

B.2 Email Server Security

As part of the system characterization, application owners should identify the role of email in transmitting election information. Specifically:

- What kind of election information will be transmitted outside the organization via email?
- What election information will be received from the public via email?
- What election information might be stored (generally only temporarily) on an email server?

B.2.1 Outbound Email Security

In most cases, the transmission of election information will bring no unique security requirements for outgoing email. The best practices described in SP800-45 will all apply to the server that process outbound email.

Because the public will consider email originating from election officials to be trusted, care should be taken to verify that only authorized entities can use the organization's outgoing email server to send messages, and that all outgoing messages are scanned for malware.

In order to increase the likelihood that election information will be correctly delivered via email and increase the likelihood that forgeries from external parties will be flagged as such, jurisdictions should configure forgery countermeasures such as Domain Keys Identified Mail (DKIM) on servers that send election materials via email. While not all voters' mail providers will recognize such protections, delivery reliability will be significantly improved when communicating with those providers that do process the additional verification data.

Organizations should ensure that all outbound email connections require authentication with at least a user name and password.

Organizations should avoid transmitting information via email if it's considered sensitive to disclosure according to local, state or federal regulations.

The outbound email server should return any error notifications it receives to the sender of the email for further analysis. Most servers will do this by default.

System owners should confirm that the maintenance process specifically ensures that malware signatures are kept current.

B.2.2 Inbound Email Security

In applications where election officials receive completed forms from voters, additional specific considerations may be relevant. In particular, users of the mail server will need to open attachments received from the public over the Internet in order to perform their job functions. This increases the organization's exposure to malware. Additionally, such completed forms are likely to be stored on a mail server at least until they have been processed. This storage may introduce specific requirements, depending on local, state or federal regulations.

Election officials should work with the IT organization to ensure that access to the mail server is sufficiently controlled to meet these requirements. It may make sense for officials who receive such information to have mailboxes located on a server dedicated to election information.

Whether or not such a dedicated server is necessary, these considerations suggest that an architecture which incorporates an incoming mail gateway is preferred when email is used for inbound election materials.

Incoming SMTP connections from the Internet should be routed through the mail gateway. The mail gateway should scan message content and filter or quarantine suspicious messages prior to delivering them to the internal mail server. If possible, this gateway should be configured to verify that attachments are of the expected type and fall into the expected size range, in addition to checking for malware. Ideally, the internal mail server should scan the message content a second time, using anti-malware software from a different source than the mail gateway. This architecture serves to reduce potential exposure to malware as well as to ensure that messages are not stored on a machine which accepts connections from an untrusted network.

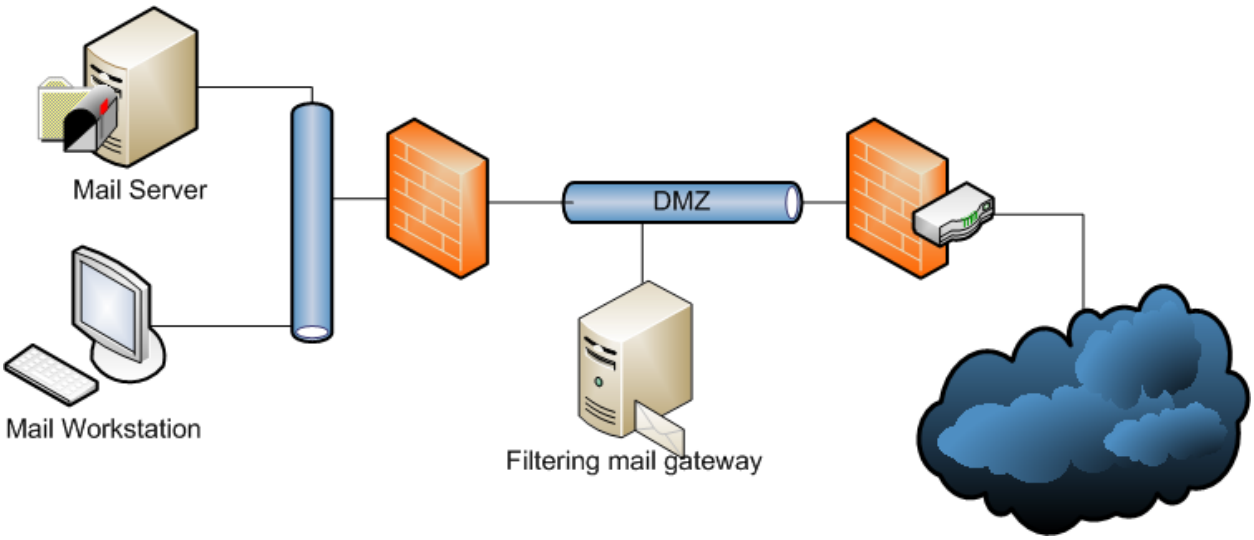

Figure 4. Comon architecture for incoming email

System owners should confirm that the maintenance process specifically ensures that malware signatures are kept up-to-date.

SP 800-45 details additional security best practices for email servers.

B.3 Email Client Security

As with other components, information categorized as part of the system characterization will determine specific email client security concerns. The best practices documented in NISTIR 7682 for workstation security and in SP 800-45 for email client security will apply to all clients. Because email clients need to interact with untrusted data, these security practices are particularly important. Care should be taken to ensure that configuration management practices are actively maintained, especially with regard to patching the OS and applications and maintaining the currency of malware signatures. Those workstations which receive completed forms as attachments, sent by the general public over the Internet, merit additional considerations.

First, it's almost inevitable that a workstation used to retrieve such email will store voter information, even if only temporarily. Election officials should verify that the workstation meets any specific local, state or federal requirements for systems used to store such information.

Additionally, since such attachments may be constantly solicited (and therefore will always be expected by the workstation operator) and are received through an untrusted channel, the risk of malware infection is

elevated. To counter this risk, election officials and administrators should verify that up-to-date, active malware protection is installed on the system. It is further beneficial if this protection uses signatures from a different source than the protection installed on the mail server.

As with all email clients, active features like scripting support, automatic opening of email and email previews should be disabled. When attachments are used, system owners should pay similar attention to disable these features in any software used to process these. So, for example, in Microsoft Word, macros should be disabled. In PDF processing software, javascript, ActiveX and the execution of external applications should be disabled. Future versions of PDF-processing software continue to incorporate additional security features. As part of the continuous monitoring process, an individual should be identified to monitor new releases of any software used to process attachments and fast-track versions with new security features into production.

To further mitigate the threat of malware, it is a good practice to use a dedicated machine for monitoring a mailbox that actively solicits messages from the general public. Sensitive data and critical applications should be kept to a minimum on this workstation, and it should not be used for other important election functions.

As with all applications, proper user training is a key factor in the security of the system. In this case, the users who retrieve and read these attachments should be trained to recognize the expected type and size of attachment and seek assistance prior to opening any that fall outside these parameters.

B.4 Web Server Security

Security considerations for Web servers will vary greatly depending on the role the server plays in delivering election information. For most systems, the Web server's role in the system will be broadly characterized in one or more of the following ways:

- Delivers non-personalized election information to the public
- Delivers personalized election information to the public
- Receives information from the public.

Certain common security practices for Web servers will apply to a server in any of these roles, including:

- Minimize software installed on the Web server
- Keep server software up-to-date
- Validate all user-supplied input

- Minimize the use of active content
- Restrict the privilege of the server process
- Separate the privileged administrator interface for managing the Web application from the unprivileged user interface.

Detailed guidelines for securing public Web servers can be found in SP 800-44. Additional general guidelines for Web application security are summarized in section 5.10 of NISTIR 7682. This section will not generally aim to repeat those, but will focus on specific concerns relative to the above functions.

B.4.1 Encryption

Because members of the public will consider the jurisdiction a trustworthy source of information, all Web servers supplying the public with election information should use Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to provide authentication of the server's identity even in cases where the information being served is not sensitive. Domain-verified TLS server certificates are available inexpensively or without cost, depending on the vendor, and will assure voters that information was not modified in transit.

Organizations should ensure that Web servers are configured to allow only NIST-approved SSL/TLS configurations. Specifically, only SSL 3.0 or later and TLS 1.0 or later should be used, and the cipher suites should be restricted to those identified in section 4 of NIST special publication 800-57 (part 3). Key sizes should be selected using the guidance in section 2 of the same special publication.

B.4.2 Delivery of Non-Personalized Information

In most cases, servers containing only non-personalized election information will not have additional specific technical concerns. Election officials should verify that proper procedures are followed for publishing this information so as to comply with relevant local, state and federal regulations. Information owners should work with IT staff to use technical controls that enforce these procedures.

B.4.3 Delivery of Personalized Information

Servers that deliver personalized information to the public may require access to information deemed sensitive. In this case, some verification that information is only being delivered to the correct individual will be required. Election officials should ensure that this verification meets applicable regulations.

If the personalized information being supplied to the voter is not public, measures should be taken to prevent automated processes from attempting to brute-force this verification process. Such measures might include:

- Challenge-response tests such as CAPTCHA which require human intervention before a server will process a request
- Limitations on the number of times a specific voter's information may be queried within a pre-determined timeframe
- Requiring the user to supply a pre-shared response sent through another channel, e.g. to a voter's previously registered email address, postal address or phone

If the Web server requires access to sensitive information, the repository (usually a database) containing this should be stored on a protected network which is not directly accessible from the Internet. An example of such an architecture is in found in the figure below.

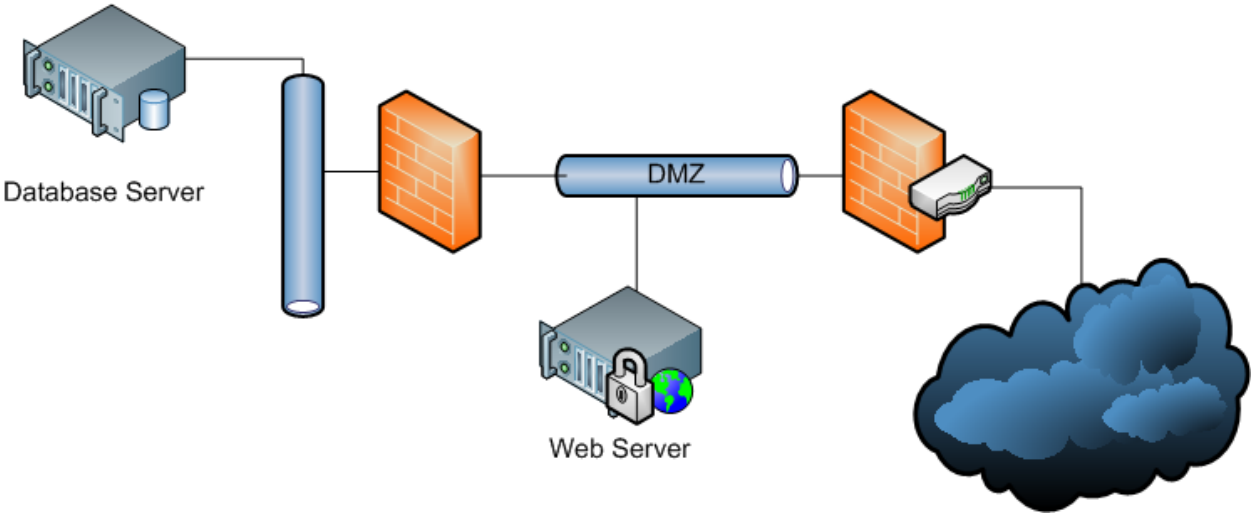

Figure 5. Common network architecture for an Internet-accessible Web server

Care should be taken to ensure that access by jurisdiction officials to any sensitive information stored in the database also complies with any relevant regulations.

B.4.4 Receipt of Information

Web servers used to receive information from the public have three unique security considerations which may vary depending on the type of information transmitted.

- Confidentiality of submitted information – If voters are submitting sensitive information to the jurisdiction using the Web server,

controls must be established to prevent this data from being improperly disclosed.

- Protection of jurisdiction systems – Submitted information must be properly validated to guard against introduction of malicious content onto the jurisdiction's protected network.
- Protection of other external system users – Information submitted by one untrusted user should not be viewable by other users.

The common security practices described in SP 800-44 and NISTIR 7682 aimed at protecting confidentiality and preventing active injection attacks (SQL injection, cross-site scripting, CSRF, etc.) all serve to address these considerations.

One common case that is of particular concern interest in the context of election systems is the submission of files for processing by election officials, especially PDF forms. When a user uploads a file, it should be quarantined in a location that is not readable by the Web server. This could be a filesystem directory to which the Web server context only has write access, a "drop box" on another server, or even a form which is submitted to a dedicated upload server. As with files received via email, these files should be scanned for malware prior to processing by election officials.

Ideally, as with email clients, initial processing of these files would occur on a workstation dedicated to this purpose. If possible, these files should be scanned for malware both at the time they are stored and at the time they are retrieved, preferably by different scanning engines. The same precautions outlined for email clients should be followed when processing received files that may contain active content.

In addition to ensuring that these files cannot be served to other Web users, officials should work with technical staff to establish controls on the file repository which limit internal access to duly authorized personnel.

Appendix C: Glossary

Access Control	The process of granting or denying specific requests for obtaining and using information and related information processing services.
Certificate	A digital representation of information which at least 1. identifies the certification authority issuing it, 2. names or identifies its subscriber, 3. contains the subscriber's public key, 4. identifies its operational period, and 5. is digitally signed by the certification authority issuing it.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates.
Commercial-Off-The-Shelf (COTS)	Hardware and software IT products that are ready-made and available for purchase by the general public.
Cross-Site Request Forgery (CSRF)	A type of Web exploit where an unauthorized party causes commands to be transmitted by a trusted user of a Web site without that user's knowledge.
Demilitarized Zone (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks.
Denial of Service (DoS)	The prevention of authorized access to resources or the delaying of time-critical operations.
Distributed Denial of Service (DDoS)	A Denial of Service technique that uses numerous hosts to perform the attack.
Hash-based Message Authentication Code (HMAC)	A message authentication code that uses a cryptographic key in conjunction with a hash function.

Identification and Authentication (I&A)	The process of establishing the identity of an entity interacting with a system.
Intrusion Detection System (IDS)	Software that looks for suspicious activity and alerts administrators.
Intrusion Prevention System (IPS)	System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
Man-In-The-Middle (MITM)	An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.
Message Authentication Code	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Metacharacter	A character that has some special meaning to a computer program and therefore will not be interpreted properly as part of a literal string.
Out Of Band	Used to refer to information transmitted through a separate communications channel.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Token	Something a user possess and controls used to authenticate the user's identity.
Transport Layer Security (TLS)	An authentication and encryption protocol widely implemented in browsers and Web servers. HTTP traffic transmitted using TLS is known as HTTPS.
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act.
UOCAVA Systems	Information technology systems which enable uniformed and overseas United States citizens to vote.

XSS	Cross-Site Scripting (XSS) is a security flaw found in some Web applications that enables unauthorized parties to cause client-side scripts to be executed by other users of the Web application.